APPENDIX [TBC] –IKI CERTIFICATE POLICY

CONTENTS

1 INTRODUCTION

The document comprising this Appendix [X] (together with its Annexes A and B):

- shall be known as the "IKI Certificate Policy" (and in this document is referred to simply as the "Policy"); and
- is a SEC Subsidiary Document related to Section L9 of the Code (The SMKI Document Set).

1.1 OVERVIEW

(A) This Policy sets out the arrangements relating to:

(i) IKI Certificates; and

(ii) IKI Certificate Authority (ICA) Certificates.

(B) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

1.2 DOCUMENT NAME AND IDENTIFICATION

(A) This Policy has been registered with the Internet Address Naming Authority and assigned an OID of 1.2.826.0.1.8641679.1.2.1.3

1.3 SMKI PARTICIPANTS

1.3.1 The IKI Root Certification Authority

(A) The definition of IKI Certification Authority is set out in Annex A.

1.3.2 Registration Authorities

(A) The definition of Registration Authority is set out in Annex A.

1.3.3 Subscribers

(A) In accordance with Section L3 of the Code (The SMKI Services), certain Parties and RDPs may become Authorised Subscribers.

(B) In accordance with Section L3 of the Code (The SMKI Services), an Authorised Subscriber shall be an Eligible Subscriber in relation to certain Certificates.

(C) The SMKI RAPP sets out the procedure to be followed by an Eligible Subscriber in order to become a Subscriber for one or more Certificates.

(D) Eligible Subscribers are subject to the applicable requirements of the SMKI RAPP and Section L11 of the Code (Subscriber Obligations).

(E) Obligations on the DCC acting in the capacity of an Eligible Subscriber are set out in Section L11 of the Code (Subscriber Obligations).

(F) The definitions of the following terms are set out in Section A of the Code (Definitions and Interpretation):

(i) Authorised Subscriber; and

(ii) Subscriber.

(G) Eligible Subscribers are defined in Annex A of this Policy

1.3.4 Subjects

(A) The Subject of an IKI Certificate may be an Individual or an Organisation and must be identified in the Subject field of the IKI Certificate Profile in accordance with Annex B

(B) The Subject of an ICA Certificate must be the entity named in the Subject field of the Root ICA Certificate Profile or Issuing ICA Certificate Profile (as the case may be) in accordance with Annex B.

(C) The definition of Subject is set out in Annex A.

1.3.5 Relying Parties

(A) In accordance with Section L12 of the Code, certain Parties may be Relying Parties.

(B) Relying Parties are subject to the applicable requirements of Section L12 of the Code (Relying Party Obligations).

(C) Obligations on the DCC acting in the capacity of a Relying Party are set out in Section L12 of the Code (Relying Party Obligations).

(D) The definition of Relying Party is set out in Annex A.

(E) The only Relying Party for IKI Certificates and ICA Certificates is the DCC in its role as the provider of the SMKI Services. No other parties should place any reliance on these credentials.

1.3.6 SMKI Policy Management Authority

(A) Provision in relation to the SMKI PMA is made in Section L1 of the Code (SMKI Policy Management Authority).

1.3.7 SMKI Repository Provider

(A) Provision in relation to the SMKI Repository Service is made in Section L5 of the Code (The SMKI Repository Service).

1.4 USAGE OF IKI CERTIFICATES AND ICA CERTIFICATES

1.4.1 Appropriate Certificate Uses

(A) The ICA shall ensure that IKI Certificates are Issued only:

(i) to Eligible Subscribers; and

(ii) for the purposes of authenticating the Subject to the SMKI Services.

(B) The ICA shall ensure that ICA Certificates are Issued only to the ICA:

(i) in its capacity as, and for the purposes of, exercising the functions of, the Root ICA; and

(ii) in its capacity as, and for the purposes of, exercising the functions of, an Issuing ICA.

(C) Further provision in relation to the use of Certificates is made in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code.

1.4.2 Prohibited Certificate Uses

(A) No Party or RDP shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

1.5 POLICY ADMINISTRATION

1.5.1 Organisation Administering the Document

(A) This Policy is a SEC Subsidiary Document and is administered as such in accordance with the provisions of the Code.

1.5.2 Contact Person

(A) Questions in relation to the content of this Policy should be addressed to the ICA or the SMKI PMA.

1.5.3 Person Determining IKI CPS Suitability for the Policy

(A) Provision is made in Section L9 of the Code (The SMKI Document Set) for the SMKI PMA to approve the IKI CPS.

1.5.4 IKI CPS Approval Procedures

(A) Provision is made in Section L9 of the Code (The SMKI Document Set) for the procedure by which the SMKI PMA may approve the IKI CPS.

1.5.5 Registration Authority Policies and Procedures

(A) The SMKI Registration Authority Policies and Procedures (the SMKI RAPP) are set out at Appendix D of the Code.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

(A) Definitions of the expressions used in this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

1.6.2 Acronyms

(A) Any acronyms used for the purposes of this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Provision is made in Section L5 of the Code (The SMKI Repository Service) for the establishment, operation and maintenance of the SMKI Repository.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

(A) The ICA shall ensure that the following are lodged in the SMKI Repository:

(i) each version of the SMKI RAPP;

(ii) the latest version of the IKI CRL;

(iii) the latest version of the IKI ARL;

(iv) each version of this Policy; and

(v) any other document or information that may from time to time be specified, for the purposes of this provision, by the SMKI PMA.

(B) The ICA may lodge in the SMKI Repository such other documents or information as it may from time to time consider appropriate.

(C) Further provision on the lodging of documents and information in the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

2.3 TIME OR FREQUENCY OF PUBLICATION

(A) The ICA shall ensure that:

(i) the SMKI RAPP is lodged in the SMKI Repository, and a revised version of the SMKI RAPP is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(ii) the IKI CRL is lodged in the SMKI Repository, and a revised version of the IKI CRL is lodged in the SMKI Repository within such time as is specified in Part 4.9.7 of this Policy;

(iii) the IKI ARL is lodged in the SMKI Repository, and a revised version of the IKI ARL is lodged in the SMKI Repository within such time as is specified in Part 4.9.7 of this Policy; and

(iv) any other document that may from time to time be specified by the SMKI PMA is lodged in the SMKI Repository within such time as may be directed by the SMKI PMA.

2.4 ACCESS CONTROLS ON REPOSITORIES

(A) Provision in relation to access controls for the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

(A) Provision is made in the SMKI RAPP to ensure that the name of the entity that is the Subject of each Certificate, Issued to DCC Registration Authority (RA) Managers, DCC RA Personnel and Authorised Responsible Officers (AROs), is in accordance with the relevant Certificate Profile at Annex B.

(B) The ICA shall ensure that the IKI CPS contains provisions to ensure that the entity that is the Subject of each Certificate Issued to other DCC Eligible Subscribers is in accordance with the relevant Certificate Profile at Annex B

3.1.2 Need for Names to be Meaningful

(A) Provision is made in the SMKI RAPP to ensure that the name of the Subject of each IKI Certificate Issued to DCC RA Managers, DCC RA Personnel and AROs, is meaningful and consistent with the relevant Certificate Profile in Annex B.

(B) The ICA shall ensure that the IKI CPS contains provisions to ensure that the name of the Subject of each IKI Certificate Issued to other DCC Eligible Subscribers is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or Pseudonymity of Subscribers

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

(i) prohibit DCC RA Managers, DCC RA Personnel and AROs from requesting the Issue of a Certificate anonymously or by means of a pseudonym; and

(ii) permit the ICA to Authenticate each DCC RA Manager, DCC RA Personnel and ARO..

(B) The ICA shall ensure that the IKI CPS contains provisions to:

(i) prohibit other DCC Eligible Subscribers from requesting the Issue of a Certificate anonymously or by means of a pseudonym; and

(ii) require the ICA to Authenticate other DCC Eligible Subscribers.

3.1.4 Rules for Interpreting Various Name Forms

(A) Provision in relation to name forms is made in Annex B.

3.1.5 Uniqueness of Names

(A) Provision in relation to the uniqueness of names is made in Annex B.

3.1.6 Recognition, Authentication, and Role of Trademarks

(A) Provision in relation to the use of trademarks, trade names and other restricted information in Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

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

(i) the procedure to be followed by an DCC RA Manager, DCC RA Personnel and AROs in order to prove its possession of the Private Key which is associated with the Public Key contained in any Certificate that is the subject of a Certificate Signing Request; and

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism.

(B) The ICA shall ensure that the IKI CPS contains provisions on:

(i) the procedure to be followed by other DCC Eligible Subscribers in order to prove its possession of the Private Key which is associated with the Public Key contained in any Certificate that is the subject of a Certificate Signing Request; and

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism.

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 ICA 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 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 or RDP shall be set to 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.

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 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.

3.2.4 Non-verified Subscriber Information

(A) The ICA shall verify all information in relation to Certificates.

(B) Further provision on the content of ICA Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2.5 Validation of Authority

See Part 3.2.2 of this Policy.

3.2.6 Criteria for Interoperation

[Not applicable in this Policy]

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The ICA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for Re-Key after Revocation

[Not applicable in this Policy]

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

3.4.1 Authentication for Certificate Revocation Requests

(A) Provision is made in the SMKI RAPP in relation to procedures designed to ensure the Authentication of persons who submit a Certificate Revocation Request and verify that they are authorised to submit that request.

4 CERTIFICATE AND LIFECYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Submission of Certificate Applications

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

(i) in respect of an IKI Certificate:

(a) the circumstances in which a DCC RA Manager, DCC RA Personnel and ARO may submit a Certificate Signing Request; and

(b) the means by which it may do so, including through the use of an authorised System; and

(B) The ICA shall ensure that the IKI CPS contains provisions:

(i) in respect of an IKI Certificate:

(a) the circumstances in which other DCC Eligible Subscribers may submit a Certificate Signing Request; and

(b) the means by which it may do so, including through the use of an authorised System.

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 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.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the SMKI RAPP in relation to the Authentication by the ICA of DCC RA Managers, DCC RA Personnel and AROs which submit a Certificate Signing Request.

(B) The ICA shall ensure that the IKI CPS contains provisions in relation to the Authentication by the ICA of other DCC Eligible Subscribers which submit a Certificate Signing Request.

4.2.2 Approval or Rejection of Certificate Applications

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

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

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

(B) Where any Certificate Signing Request satisfies the requirements set out in the SMKI RAPP, this Policy or any other provision of the Code, the ICA shall Issue the Certificate which was the subject of the Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(A) The ICA shall ensure that it processes all Certificate Signing Requests relating to IKI Certificates promptly, and in any event in accordance with such time as is specified in the SMKI RAPP. .

4.3 CERTIFICATE ISSUANCE

4.3.1 ICA Actions during Certificate Issuance

(A) The ICA may Issue a Certificate only:

(i) in accordance with the provisions of this Policy; and

(ii) in response to a Certificate Signing Request made by an Eligible Subscriber in accordance with this Policy.

(B) The ICA shall ensure that:

(i) each ICA Certificate Issued by it contains information that it has verified to be correct and complete; and

(ii) each IKI Certificate Issued by it contains information consistent with the information in the Certificate Signing Request.

(C) An ICA Certificate may only be:

(i) Issued by the ICA; and

(ii) for that purpose, signed using the Root ICA Private Key.

(D) An IKI Certificate may only be:

(i) Issued by the ICA; and

(ii) for that purpose, signed using an Issuing ICA Private Key.

(E) The ICA shall not Issue:

(i) an Issuing ICA Certificate using a Root ICA Private Key after the expiry of the Validity Period of a Root ICA Certificate containing the Public Key associated with that Private Key; or

(ii) an IKI Certificate using an Issuing ICA Private Key after the expiry of the Validity Period of an Issuing ICA Certificate containing the Public Key associated with that Private Key.

4.3.2 Notification to Eligible Subscriber by the ICA of Issuance of Certificate

(A) Provision is made in the SMKI RAPP for the ICA to notify DCC RA Manager, DCC RA Personnel and ARO where that DCC RA Manager, DCC RA Personnel or AROs is Issued with a Certificate which was the subject of a Certificate Signing Request made by them.

(B) The ICA shall ensure the IKI CPS includes provisions for the ICA to notify other DCC Eligible Subscribers where that other DCC Eligible Subscriber is Issued with a Certificate which was the subject of a Certificate Signing Request made by them.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

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

(i) specify a means by which a DCC RA Manager, DCC RA Personnel or ARO may clearly indicate to the ICA its rejection of a Certificate which has been Issued to them; and

(ii) ensure that each DCC RA Manager, DCC RA Personnel or ARO to which a Certificate has been Issued, and which has not been rejected, is treated as having accepted that Certificate.

(B) The ICA shall ensure the IKI CPS includes provisions that:

(i) specify a means by which any other DCC Eligible Subscriber may clearly indicate to the ICA it rejection of a Certificate which has been Issued to them; and

(ii) ensure that each Eligible Subscriber to which a Certificate has been Issued, and which has not been rejected, is treated as having accepted that Certificate.

(B) A Certificate which has been Issued by the ICA shall not be treated as valid for any purposes of this Policy or the Code until it is treated as having been accepted by the Eligible Subscriber to which it was Issued.

(C) The ICA shall maintain a record of all Certificates which have been Issued by it and are treated as accepted by a Subscriber.

(D) Further provision in relation to the rejection and acceptance of Certificates is made in Section L11 of the Code (Subscriber Obligations).

4.4.2 Publication of Certificates by the ICA

[Not applicable to this Policy]

4.4.3 Notification of Certificate Issuance by the ICA to Other Entities

(A) The ICA shall give notice of the Issue of a Certificate only to the Eligible Subscriber which submitted a Certificate Signing Request in respect of that Certificate.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

(A) Provision for restrictions on the use by Subscribers of Private Keys in respect of Certificates is made in:

(i) Section L11 of the Code (Subscriber Obligations); and

(ii) this Policy.

4.5.2 Relying Party Public Key and Certificate Usage

(A) Provision in relation to reliance that may be placed on a Certificate is made in Section L12 of the Code (Relying Party Obligations).

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances of Certificate Renewal

(A) This Policy does not support the renewal of Certificates.

(B) The ICA may only replace, and shall not renew, any Certificate.

4.6.2 Circumstances of Certificate Replacement

(A) Where any ICA System or any ICA Private Key is (or is suspected by the ICA of being) Compromised, the ICA shall:

(i) immediately notify the SMKI PMA;

(ii) provide the SMKI PMA with all of the information known to it in relation to the nature and circumstances of the event of Compromise or suspected Compromise; and

(iii) where the Compromise or suspected Compromise relates to an ICA Private Key:

(a) ensure that the Private Key is no longer used;

(b) promptly notify each of the Subscribers for any IKI Certificates Issued using that Private Key; and

(c) promptly notify the SMKI PMA, verifiably destroy the ICA Private Key Material and revoke the corresponding ICA Certificate.

(B) Where the ICA Root Private Key is Compromised (or is suspected by the ICA of being Compromised), the ICA:

(i) may issue a replacement for any ICA Certificate that has been Issued using that Private Key; and

(ii) shall ensure that the Subscriber for that ICA Certificate both applies for the Issue of a new Certificate in accordance with this Policy and revokes that ICA Certificate.

(C) The ICA shall ensure that a replacement for each ICA Certificate is Issued prior to end of the Validity Period of that ICA Certificate.

(D) A Subscriber for an IKI Certificate may request a replacement for that Certificate at any time by applying for the Issue of a new IKI Certificate in accordance with this Policy and, where this replacement is for purposes other than to replace an expiring Certificate, shall submit a Certificate Revocation Request in respect of the replaced IKI Certificate.

4.6.3 Who May Request a Replacement Certificate

See Part 4.1 of this Policy.

4.6.4 Processing Replacement Certificate Requests

See Part 4.2 of this Policy.

4.6.5 Notification of Replacement Certificate Issuance to a Subscriber

See Part 4.3.2 of this Policy.

4.6.6 Conduct Constituting Acceptance of a Replacement Certificate

See Part 4.4.1 of this Policy.

4.6.7 Publication of a Replacement Certificate by the ICA

[Not applicable in this Policy]

4.6.8 Notification of Certificate Issuance by the ICA to Other Entities

[Not applicable in this Policy]

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstances for Certificate Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The ICA shall not provide a Certificate Re-Key service.

(C) Where a new Key Pair has been generated, the Subscriber shall apply for a new Certificate in accordance with this Policy.

4.7.2 Who may Request Certification of a New Public Key

[Not applicable to this Policy]

4.7.3 Processing Certificate Re-Keying Requests

[Not applicable to this Policy]

4.7.4 Notification of New Certificate Issuance to Subscriber

[Not applicable to this Policy]

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[Not applicable to this Policy]

4.7.6 Publication of the Re-Keyed Certificate by the ICA

[Not applicable to this Policy]

4.7.7 Notification of Certificate Issuance by the ICA to Other Entities

[Not applicable to this Policy]

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification.

(B) Neither the ICA nor any Subscriber may modify a Certificate.

4.8.2 Who may request Certificate Modification

[Not applicable to this Policy]

4.8.3 Processing Certificate Modification Requests

[Not applicable to this Policy]

4.8.4 Notification of New Certificate Issuance to Subscriber

[Not applicable to this Policy]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[Not applicable to this Policy]

4.8.6 Publication of the Modified Certificate by the ICA

[Not applicable to this Policy]

4.8.7 Notification of Certificate Issuance by the ICA to Other Entities

[Not applicable to this Policy]

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

(A) A Subscriber shall ensure that it submits a Certificate Revocation Request in relation to a Certificate:

(i) immediately upon becoming aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate;

(ii) when any of the permitted reasons for revocation of authentication credentials, as set out in the SMKI RAPP, are met; or

(ii) immediately upon ceasing to be an Eligible Subscriber in respect of that Certificate.

(B) The ICA must revoke a Certificate upon:

(i) receiving a Certificate Revocation Request if the Certificate to which that request relates has been Authenticated in accordance with Part 3.4.1 of this Policy; or

(ii) being directed to do so by the SMKI PMA.

(C) The ICA must revoke a Certificate in relation to which it has not received a Certificate Revocation Request:

(i) where it becomes aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate; or

(ii) where it becomes aware that the Subscriber for that Certificate has ceased to be an Eligible Subscriber in respect of the Certificate.

(D) In an extreme case, where it considers it necessary to do so for the purpose of preserving the integrity of the SMKI Services, the ICA may, on the receipt of a Certificate Revocation Request in relation to a Certificate which has not been Authenticated in accordance with Part 3.4.1 of this Policy, revoke that Certificate.

(E) Where the ICA revokes a Certificate in accordance with paragraph (D) it shall notify the SMKI PMA and provide a statement of its reasons for the revocation.

4.9.2 Who can Request Revocation

(A) Any Subscriber may submit a Certificate Revocation Request in relation to a Certificate for which it is the Subscriber, and shall on doing so:

(i) provide all the information specified in the SMKI RAPP (including all the information necessary for the Authentication of the Certificate); and

(ii) specify its reason for submitting the Certificate Revocation Request (which shall be a reason consistent with Part 4.9.1(A) of this Policy).

(B) The SMKI PMA may direct the ICA to revoke a Certificate.

(C) The ICA may elect to revoke a Certificate in accordance with Part 4.9.1(D) of this Policy.

4.9.3 Procedure for Revocation Request

(A) Provision is made in the SMKI RAPP in relation to the procedure for submitting and processing a Certificate Revocation Request associated with Certificates Issued to DCC Registration Authority (RA) Managers, DCC RA Personnel, Authorised Responsible Officers (AROs).

(B) The ICA shall ensure that the IKI CPS contains provisions in relation to the procedure for submitting and processing a Certificate Revocation Request associated with Certificates Issued to other DCC Eligible Subscribers.

(C) On receiving a Certificate Revocation Request, the ICA shall use its reasonable endeavours to:

(i) Authenticate the Subscriber making that request;

(ii) Authenticate the Certificate to which the request relates; and

(iii) confirm that a reason for the request has been specified in accordance with Part 4.9.2 of this Policy.

(D) Where the ICA, in accordance with Part 4.9.1(C) of this Policy, intends to revoke a Certificate in relation to which it has not received a Certificate Revocation Request, it shall use its best endeavours prior to revocation to confirm with the Subscriber for that Certificate the circumstances giving rise to the revocation.

(E) The ICA shall inform the Subscriber for a Certificate where that Certificate has been revoked.

4.9.4 Revocation Request Grace Period

[Not applicable in this Policy]

4.9.5 Time within which ICA must process the Revocation Request

(A) The ICA shall ensure that it processes all Certificate Revocation Requests promptly, and in any event in accordance with such time as is specified in the SMKI RAPP.

4.9.6 Revocation Checking Requirements for Relying Parties

(A) Provision in relation to the revocation checking requirements for Relying Parties is made in Section L12 of the Code (Relying Party Obligations).

4.9.7 CRL Issuance Frequency (if applicable)

(A) The ICA shall ensure that an up to date version of the IKI ARL is lodged in the SMKI Repository:

(i) at least once in every period of twelve months; and

(ii) promptly on the revocation of an ICA Certificate.

(B) Each version of the IKI ARL shall be valid until the date which is 12 months after the date on which that version of the IKI ARL is lodged in the SMKI Repository.

(C) Further provision in relation to the reliance that may be placed on the IKI ARL (and on versions of it) is set out in Section L12 of the Code (Relying Party Obligations).

(D) The ICA shall ensure that an up to date version of the IKI CRL is lodged in the SMKI Repository:

(i) at least once in every period of twelve hours; and

(ii) within one hour on the revocation of an IKI Certificate.

(E) Each version of the IKI CRL shall be valid until 48 hours from the time at which it is lodged in the SMKI Repository.

(F) Further provision in relation to the reliance that may be placed on the IKI CRL (and on versions of it) is set out in Section L12 of the Code (Relying Party Obligations).

(G) The ICA shall ensure that each up to date version of the IKI ARL and IKI CRL:

(i) continues to include each relevant revoked Certificate until such time as the Validity Period of that Certificate has expired; and

(ii) does not include any revoked Certificate after the Validity Period of that Certificate has expired.

(H) The ICA shall ensure that the IKI CRL contains a non-critical entry extension which identifies the reason for the revocation of each Certificate listed on it in accordance with RFC 5280 (section 5.3.1).

(I) The ICA shall retain a copy of the information contained in all versions of the IKI CRL and IKI ARL, together with the dates and times between which each such version was valid. This information shall be made available as soon as is reasonably practicable, on receipt of a request, to the Panel, the SMKI PMA, any Subscriber or any Relying Party.

4.9.8 Maximum Latency for CRLs (if applicable)

See Part 4.9.7 of this Policy.

4.9.9 On-line Revocation/Status Checking Availability

(A) This Policy does not support on-line revocation status checking.

(B) The ICA shall not provide any on-line revocation status checking service.

4.9.10 On-line Revocation Checking Requirements

[Not applicable in this Policy]

4.9.11 Other Forms of Revocation Advertisements Available

[Not applicable in this Policy]

4.9.12 Special Requirements in the Event of Key Compromise

See Part 4.6.2 of this Policy.

4.9.13 Circumstances for Suspension

[Not applicable in this Policy]

4.9.14 Who can Request Suspension

[Not applicable in this Policy]

4.9.15 Procedure for Suspension Request

[Not applicable in this Policy]

4.9.16 Limits on Suspension Period

[Not applicable in this Policy]

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

[Not applicable in this Policy]

4.10.2 Service Availability

(A) In circumstances in which:

(i) an up to date version of the IKI ARL has not been lodged in the SMKI Repository in accordance with Part 4.9.7(A) of this Policy; or

(ii) the SMKI Repository Service is unavailable,

a Relying Party shall be entitled to rely on the IKI ARL for the period during which it remains valid in accordance with the provisions of Part 4.9.7(B) of this Policy, but thereafter shall not rely on any Certificate.

(B) In circumstances in which:

(i) an up to date version of the IKI CRL has not been lodged in the SMKI Repository in accordance with Part 4.9.7(C) of this Policy; or

(ii) the SMKI Repository Service is unavailable,

a Relying Party shall be entitled to rely on the IKI CRL for the period during which it remains valid in accordance with the provisions of Part 4.9.7(D) of this Policy, but thereafter shall not rely on any IKI Certificate.

4.10.3 Optional Features

[Not applicable in this Policy]

4.11 END OF SUBSCRIPTION

[Not applicable in this Policy]

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policies and Practices

(A) This Policy does not support Key Escrow.

(B) The ICA shall not provide any Key Escrow service.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

[Not applicable in this Policy]

5 FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

(A) The ICA shall ensure that the ICA 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 ICA shall ensure that:

(i) all of the physical locations in which the ICA 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 ICA shall ensure that the ICA Systems cannot be indirectly accessed from any location outside the United Kingdom.

(D) The ICA shall ensure that the IKI 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:

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

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

5.1.2 Physical Access

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to access control, including in particular provisions designed to:

(i) establish controls such that only appropriately authorised personnel may have unescorted physical access to ICA Systems or any System used for the purposes of Time-Stamping;

(ii) ensure that any unauthorised personnel may have physical access to such Systems only if appropriately authorised and supervised;

(iii) ensure that a site access log is both maintained and periodically inspected for all locations at which such Systems are sited; and

(iv) ensure that all removable media which contain sensitive plain text Data and are kept at such locations are stored in secure containers accessible only to appropriately authorised individuals.

5.1.3 Power and Air Conditioning

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the ICA Systems are situated.

5.1.4 Water Exposure

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to water exposure at all physical locations in which the ICA Systems are situated.

5.1.5 Fire Prevention and Protection

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the ICA Systems are situated.

5.1.6 Media Storage

(A) The ICA shall ensure that the IKI CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions as the ICA.

5.1.7 Waste Disposal

(A) The ICA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the ICA are disposed of only using secure methods of disposal in accordance with:

(i) Information Assurance Standard No. 5:2011 (Secure Sanitisation); or

(ii) any equivalent to that Information Assurance Standard which updates or replaces it from time to time.

5.1.8 Off-Site Back-Up

(A) The ICA shall regularly carry out a Back-Up of:

(i) all Data held on the ICA Systems which are critical to the operation of those Systems or continuity in the provision of the SMKI Services; and

(ii) all other sensitive Data.

(B) For the purposes of paragraph (A), the ICA shall ensure that the IKI CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The ICA shall ensure that Data which are Backed-Up in accordance with paragraph (A):

(i) are stored on media that are located in physically secure facilities in different locations to the sites at which the Data being Backed-Up are ordinarily held;

(ii) are protected in accordance with the outcome of a risk assessment which is documented in the IKI CPS, including when being transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise ICA Private Key Material, are Backed-Up:

(a) using the proprietary Back-Up mechanisms specific to the relevant Cryptographic Module; and

(b) in a manner that is 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).

(D) The ICA shall ensure that, where any elements of the ICA Systems, any Data held for the purposes of providing the SMKI Services, or any items of ICA equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

(A) The ICA shall ensure that:

(i) no individual may carry out any activity which involves access to resources, or Data held on, the ICA Systems unless that individual has been expressly authorised to have such access;

(ii) each member of ICA Personnel has a clearly defined level of access to the ICA Systems and the premises in which they are located;

(iii) no individual member of ICA Personnel is capable, by acting alone, of engaging in any action by means of which the ICA Systems may be Compromised to a material extent; and

(iv) the IKI CPS incorporates provisions designed to ensure that appropriate controls are in place for the purposes of compliance by the ICA with the requirements of this paragraph.

5.2.2 Number of Persons Required per Task

(A) The ICA shall ensure that the IKI CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of ICA Personnel; and

(ii) the application of controls to the actions of all members of ICA Personnel who are Privileged Persons, in particular:

(a) identifying any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions; and

(b) providing that the revocation of any ICA Certificate is one such function.

(B) The ICA shall ensure that the IKI CPS, as a minimum, makes provision for the purposes of paragraph (A) in relation to the following roles:

(i) ICA Systems administration;

(ii) ICA Systems operations;

(iii) ICA Systems security; and

(iv) ICA Systems auditing.

5.2.3 Identification and Authentication for Each Role

See Part 5.2.2 of this Policy.

5.2.4 Roles Requiring Separation of Duties

See Part 5.2.2 of this Policy.

5.3 PERSONNEL CONTROLS

5.3.1 Qualification, Experience and Clearance Requirements

(A) The ICA shall ensure that all ICA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions relevant to their roles;

(iii) have received appropriate training with respect to their duties;

(iv) be bound by contract not to disclose any confidential, sensitive, personal or security-related Data except to the extent necessary for the performance of their duties or for the purposes of complying with any requirement of law; and

(v) in so far as can reasonably be ascertained by the ICA, not have been previously relieved of any past assignment (whether for the ICA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The ICA shall ensure that all ICA Personnel have, as a minimum, passed a Security Check before commencing their roles.

5.3.2 Background Check Procedures

See Part 5.3.1 of this Policy.

5.3.3 Training Requirements

See Part 5.3.1 of this Policy.

5.3.4 Retraining Frequency and Requirements

(A) The ICA shall ensure that the IKI CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of ICA Personnel.

5.3.5 Job Rotation Frequency and Sequence

(A) The ICA shall ensure that the IKI CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by members of ICA Personnel.

5.3.6 Sanctions for Unauthorised Actions

(A) The ICA shall ensure that the IKI CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by members of ICA Personnel.

5.3.7 Independent Contractor Requirements

(A) In accordance with the provisions of the Code, references to the ICA in this Policy include references to persons with whom the ICA contracts in order to secure performance of its obligations as the ICA.

5.3.8 Documentation Supplied to Personnel

(A) The ICA shall ensure that all ICA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;

(ii) the IKI CPS; and

(iii) any supporting documentation, statutes, policies or contracts.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

(A) The ICA shall ensure that:

(i) the ICA Systems record all systems activity in an audit log;

(ii) the IKI CPS incorporates a comprehensive list of all events that are to be recorded in an audit log in relation to:

(a) the activities of ICA Personnel;

(b) the use of ICA equipment;

(c) the use of (including both authorised and unauthorised access, and attempted access to) any premises at which functions of the ICA are carried out;

(d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the ICA Systems audit log); and

(iii) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of Processing Log

(A) The ICA shall ensure that:

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

(ii) all ICA 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 ICA 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;

(B) The ICA shall ensure that the IKI 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 ICA shall ensure that the IKI 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 ICA Personnel who are performing a dedicated system audit role.

5.4.3 Retention Period for Audit Log

(A) The ICA shall:

(i) retain the Audit Log so that it incorporates, on any given date, a record of all system events occurring during a period of at least twelve months prior to that date; and

(ii) ensure that a copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period is archived in accordance with the requirements of Part 5.5 of this Policy.

5.4.4 Protection of Audit Log

(A) The ICA shall ensure that:

(i) to the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance 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

(ii) to the extent to which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log Back-Up Procedures

(A) The ICA shall ensure that the Data contained in the Audit Log are Backed-Up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):

(i) on a daily basis; or

(ii) if activity has taken place on the ICA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The ICA shall ensure that all Data contained in the Audit Log which are Backed-Up are, during Back-Up:

(i) held in accordance with the outcome of a risk assessment which is documented in the IKI CPS; and

(ii) protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit Collection System (Internal or External)

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to Event-Causing Subject

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability Assessments

(A) Provision is made in Sections G2.13 to G2.14 of the Code (Management of Vulnerabilities) in relation to the carrying out of vulnerability assessments in respect of the ICA Systems.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

(A) The ICA shall ensure that it archives:

(i) the Audit Log in accordance with Part 5.4.3 of this Policy;

(ii) its records of all Data submitted to it by Eligible Subscribers for the purposes of Certificate Signing Requests; and

(iii) any other Data specified in this Policy or the Code as requiring to be archived in accordance with this Part 5.5.

5.5.2 Retention Period for Archive

(A) The ICA shall ensure that all Data which are Archived are retained for a period of at least seven years from the date on which they were Archived.

5.5.3 Protection of Archive

(A) The ICA shall ensure that Data held in its Archive are:

(i) protected against any unauthorised access;

(ii) adequately protected against environmental threats such as temperature, humidity and magnetism; and

(iii) incapable of being modified or deleted.

5.5.4 Archive Back-Up Procedures

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to its procedures for the Back-Up of its Archive.

5.5.5 Requirements for Time-Stamping of Records

(A) Provision in relation to Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive Collection System (Internal or External)

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Archive.

5.5.7 Procedures to Obtain and Verify Archive Information

(A) The ICA shall ensure that:

(i) Data held in the Archive are stored in a readable format during their retention period; and

(ii) those Data remains accessible at all times during their retention period, including during any period of interruption, suspension or cessation of the ICA's operations.

(B) The ICA shall ensure that the IKI CPS incorporates provisions in relation to the periodic verification by the ICA of the Data held in the Archive.

5.6 KEY CHANGEOVER

5.6.1 IKI Certificate Key Changeover

(A) The ICA shall Issue a new IKI Certificate in relation to a Subject where a new Certificate Signing Request is submitted by an Eligible Subscriber in accordance with the requirements of the SMKI RAPP and this Policy.

5.6.2 ICA Key Changeover

(A) Where the ICA ceases to use an ICA Private Key in accordance with the requirements of Part 4.3.1(E) of this Policy, it shall:

(i) either:

(a) verifiably destroy the ICA Private Key Material; or

(b) retain the ICA Private Key Material in such a manner that it is adequately protected against being put back into use;

(ii)

(ii) generate a new Key Pair;

(iii) ensure that any relevant Certificate subsequently Issued by it is Issued using the ICA Private Key from the newly-generated Key Pair:

(a) until the time determined in accordance with Part 4.3.1(E) of this Policy; and

(b) subject to the provisions of Part 5.7.1(C) of this Policy; and

(iv) in its capacity as the Root ICA Issue a new relevant ICA Certificate.

(B) The ICA shall ensure that the actions taken by it in accordance with the requirements of paragraph (A) are managed so as to prevent any disruption to the provision of the SMKI Services.

5.6.3 Subscriber Key Changeover

(A) Where:

(i) a Certificate has been revoked in accordance with Part 4.9 of this Policy; and

(ii) the Subscriber for that Certificate submits to the ICA a Certificate Signing Request for the Issue of a replacement Certificate,

the ICA shall verify that the reasons for the revocation and replacement of the previous Certificate have been satisfactorily addressed, and may Issue a Certificate in accordance with the Certificate Signing Request only after it has done so.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

(A) The ICA shall ensure that the IKI CPS incorporates a business continuity plan which shall be designed to ensure:

(i) continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the SMKI Services in the event of any Compromise of the ICA Systems or major failure in the ICA processes; and

(ii) that priority is given to maintain continuity in, or to recovering the capacity for, the revocation of Certificates and the making available of an up to date IKI ARL and IKI CRL.

(B) The ICA shall ensure that the procedures set out in the business continuity plan are:

(i) compliant with ISO 22301 and ISO 27031 (or any equivalent to those standards which update or replace them from time to time); and

(ii) tested periodically, and in any event at least once in each year, in order to ensure that they are operationally effective.

(C) The ICA shall ensure that the IKI CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any ICA Private Key or any part of the ICA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The ICA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy incorporates provisions setting out the steps to be taken in the event of any loss of or corruption to computing resources, software or Data.

5.7.3 Entity Private Key Compromise Procedures

See Part 5.7.1 of this Policy.

5.7.4 Business Continuity Capabilities after a Disaster

(A) The ICA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy is designed to ensure the recovery of the provision of the SMKI Services within not more than 12 hours of the occurrence of any event causing discontinuity.

5.8 CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY TERMINATION

[Not applicable in this Policy]

6 TECHNICAL SECURITY CONTROLS

The ICA shall ensure that the IKI CPS incorporates detailed provision in relation to the technical controls to be established and operated for the purposes of the exercise of its functions as the Root ICA the Issuing ICA and the Registration Authority.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(A) The ICA shall ensure that all ICA Keys are generated:

(i) in a protected environment 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);

(ii) using multi-person control, such that no single Privileged Person is capable of generating any ICA Key; and

(iii) using random numbers of such length as to make it computationally infeasible to regenerate them even with knowledge of when and by means of which equipment they were generated.

(B) The ICA shall not generate any Private Key or Public Key other than an ICA Key.

6.1.2 Private Key Delivery to Subscriber

(A) In accordance with Part 6.1.1(B), the ICA shall not generate any Private Key for delivery to a Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

(A) The ICA shall ensure that the IKI CPS incorporates provisions:

(i) in relation to the mechanism by which Public Keys of Subscribers are delivered to it for the purpose of the exercise of its functions as the Root ICA and Issuing ICA; and

(ii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10.

6.1.4 ICA Public Key Delivery to Relying Parties

[Not applicable to this Policy]

6.1.5 Key Sizes

(A) The ICA and every Subscriber shall ensure that all Private Keys and Public Keys which each of them may use for the purposes of this Policy are of the following size and characteristics

(i) 4096-bit RSA for the Root Certificate, or 2048-bit RSA for all subordinate Certificates including the Issuing ICA Certificate; and

(ii) SHA256-with-RSA Encryption as specified in RFC4055.

6.1.6 Public Key Parameters Generation and Quality Checking

(A) The ICA shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

(B) Each Subscriber shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

(A) The ICA shall ensure that each Certificate that is Issued by it has a 'keyUsage' field in accordance with RFC5280.

(B) The ICA shall ensure that each IKI Certificate that is Issued by it has a 'keyUsage' of 'digitalSignature'. (C) The ICA shall ensure that each ICA Certificate that is Issued by it has a 'keyUsage' of either:

(i) 'keyCertSign'; or

(ii) 'CRLSign'.

(D) The ICA shall ensure that no 'keyUsage' values may be set in an IKI Certificate or ICA Certificate other than in accordance with this Part 6.1.7.

6.1.8 Extended Key Usage Purposes

(A) The ICA shall ensure that each Certificate that is Issued by it has an 'extendedkeyUsage' field in accordance with RFC5280.

(B) The ICA shall ensure that each IKI Certificate that is Issued by it has an 'extendedKeyUsage' set to 'clientAuth'.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

(A) The ICA shall ensure that all ICA Private Keys shall be:

(i) protected to a high standard of assurance by physical and logical security controls; and

(ii) stored in and operated from within a Cryptographic Module which is 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).

(B) The ICA shall ensure that all ICA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated from within a Cryptographic Module which is 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).

(C) The ICA shall ensure that no ICA Private Key shall be made available in either complete or unencrypted form except in a Cryptographic Module which is 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).

(D) The ICA shall ensure that any Cryptographic Module which is used for any purpose related to Certificate life-cycle management shall:

(i) operate so as to block access to itself following a number of failed consecutive attempts to access it using Activation Data, where that number shall be set out in the IKI CPS; and

(ii) require to be unblocked by an authorised member of ICA Personnel who has been Authenticated as such following a process which shall be set out in the IKI CPS.

6.2.2 Private Key (m out of n) Multi-Person Control

See Part 6.1.1 of this Policy.

6.2.3 Private Key Escrow

(A) This Policy does not support Key Escrow.

(B) The ICA shall not provide any Key Escrow service.

6.2.4 Private Key Back-Up

(A) The ICA may Back-Up ICA Private Keys insofar as:

(i) each Private Key is protected to a standard which is at least equivalent to that required in relation to the principal Private Key in accordance with this Policy; and

(ii) where more than one Private Key is Backed-Up within a single security environment, each of the Private Keys which is Backed-Up within that environment must be protected to a standard which is at least equivalent to that required in relation to an Issuing ICA Private Key in accordance with this Policy.

6.2.5 Private Key Archival

(A) The ICA shall ensure that no ICA Key which is a Private Key is archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The ICA shall ensure that no ICA Private Key is transferred or copied other than:

(i) for the purposes of:

(a) Back-Up; or

(b) establishing an appropriate degree of resilience in relation to the provision of the SMKI Services;

(ii) in accordance with a level of protection which is 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).

6.2.7 Private Key Storage on Cryptographic Module

See Part 6.2.1 of this Policy.

6.2.8 Method of Activating Private Key

(A) The ICA shall ensure that the Cryptographic Module in which any ICA Private Key is stored may be accessed only by an authorised member of ICA Personnel who has been Authenticated following an Authentication process which:

(i) has an appropriate level of strength to ensure the protection of the Private Key; and

(ii) involves the use of Activation Data.

6.2.9 Method of Deactivating Private Key

(A) The ICA shall ensure that any ICA Private Key shall be capable of being de-activated by means of the ICA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; and

(ii) a period of inactivity of a length which shall be set out in the IKI CPS.

6.2.10 Method of Destroying Private Key

(A) The ICA shall ensure that the IKI CPS incorporates provisions for the exercise of strict controls in relation to the destruction of ICA Keys.

(B) The ICA shall ensure that no ICA Key (whether in active use, existing as a copy for the purposes of resilience, or Backed-Up) is destroyed except in accordance with a positive decision by the ICA to destroy it.

6.2.11 Cryptographic Module Rating

See Part 6.2.1 of this Policy.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

(A) The ICA shall ensure that it archives ICA Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

(A) The ICA shall ensure that the Validity Period of each Certificate Issued by it shall be as follows:

(i) in the case of an IKI Certificate, 10 years;

(ii) in the case of an Issuing ICA Certificate, 25 years; and

(iii) in the case of a Root ICA Certificate, 50 years.

(B) For the purposes of paragraph (A), the ICA shall set the 'notAfter' value specified in Annex B in accordance with that paragraph.

(C) The ICA shall ensure that no ICA Private Key is used after the end of the Validity Period of the Certificate containing the Public Key which is associated with that Private Key.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

(A) The ICA shall ensure that any Cryptographic Module within which an ICA Key is held has Activation Data that are unique and unpredictable.

(B) The ICA shall ensure that:

(i) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the ICA Keys; and

(ii) where the Activation Data comprise any PINs, passwords or pass-phrases, the ICA shall have the ability to change these at any time.

6.4.2 Activation Data Protection

(A) The ICA shall ensure that the IKI CPS incorporates provision for the use of such cryptographic protections and access controls as are appropriate to protect against the unauthorised use of Activation Data.

6.4.3 Other Aspects of Activation Data

[Not applicable in this Policy]

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to the identification and implementation, following the conclusion of any threat assessment, of security measures which make provision for at least the following:

(i) the establishment of access controls in relation to the activities of the ICA;

(ii) the appropriate allocation of responsibilities to Privileged Persons;

(iii) the identification and Authentication of organisations, individuals and Systems involved in ICA activities;

(iv) the use of cryptography for communication and the protection of Data stored on the ICA Systems;

(v) the audit of security related events; and

(vi) the use of recovery mechanisms for ICA Keys.

6.5.2 Computer Security Rating

(A) The ICA shall ensure that the IKI CPS incorporates provisions relating to the appropriate security rating of the ICA Systems.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

(A) The ICA shall ensure that any software which is developed for the purpose of establishing a functionality of the ICA Systems shall:

(i) take place in a controlled environment that is sufficient to protect against the insertion into the software of malicious code;

(ii) be undertaken by a developer which has a quality system that is:

(a) compliant with recognised international standards (such as ISO 9001:2000 or an equivalent standard); or

(b) available for inspection and approval by the SMKI PMA, and has been so inspected and approved.

6.6.2 Security Management Controls

(A) The ICA shall ensure that the IKI CPS incorporates provisions which are designed to ensure that the ICA Systems satisfy the requirements of Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

6.6.3 Life-Cycle Security Controls

See Part 6.6.2 of this Policy.

6.7 NETWORK SECURITY CONTROLS

6.7.1 Use of Offline Root ICA

(A) The ICA shall ensure that its functions as the Root ICA are carried out on a part of the ICA Systems that is neither directly nor indirectly connected to any System which is not a part of the ICA Systems.

6.7.2 Protection Against Attack

(A) The ICA shall use its best endeavours to ensure that the ICA Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:

(i) any Denial of Service Event; and

(ii) any unauthorised attempt to connect to them.

(B) The ICA shall use its reasonable endeavours to ensure that the ICA Systems cause or permit to be open at any time only those network ports, and allow only those protocols, which are required at that time for the effective operation of those Systems, and block all network ports and protocols which are not so required.

6.7.3 Separation of Issuing ICA

(A) The DCC shall ensure that, where its functions as the Issuing ICA are carried out on a part of the ICA Systems that is connected to an external network, they are carried out on a System that is Separated from all other ICA Systems.

6.7.4 Health Check of ICA Systems

(A) The ICA shall ensure that, in relation to the ICA Systems, a vulnerability assessment in accordance with Section G2.13 of the Code (Management of Vulnerabilities) is carried out with such frequency as may be specified from time to time by the Independent SMKI Assurance Service Provider.

6.8 TIME-STAMPING

6.8.1 Use of Time-Stamping

(A) The ICA shall ensure that Time-Stamping takes place in relation to all Certificates and all other ICA activities which require an accurate record of time.

(B) The ICA shall ensure that the ICA incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority which carries out Time-Stamping on behalf of the ICA.

7 CERTIFICATE CRL AND OCSP CONTROLS

7.1 CERTIFICATE PROFILES

The ICA shall use only the Certificate Profiles in Annex B.

7.1.1 Version Number(s)

[Not applicable in this Policy]

7.1.2 Certificate Extensions

[Not applicable in this Policy]

7.1.3 Algorithm Object Identifiers

[Not applicable in this Policy]

7.1.4 Name Forms

[Not applicable in this Policy]

7.1.5 Name Constraints

[Not applicable in this Policy]

7.1.6 Certificate Policy Object Identifier

[Not applicable in this Policy]

7.1.7 Usage of Policy Constraints Extension

[Not applicable in this Policy]

7.1.8 Policy Qualifiers Syntax and Semantics

[Not applicable in this Policy]

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

[Not applicable in this Policy]

7.2 CRL PROFILE

7.2.1 Version Number(s)

(A) The ICA shall ensure that the IKI ARL and IKI CRL conform with X.509 v2 and IETF RFC 5280.

7.2.2 CRL and CRL Entry Extensions

(A) The ICA shall notify Parties of the profile of the IKI CRL and of any IKI CRL extensions.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

[Not applicable in this Policy]

7.3.2 OCSP Extensions

[Not applicable in this Policy]

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.4 TOPICS COVERED BY ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.6 COMMUNICATION OF RESULTS

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

9 OTHER BUSINESS AND LEGAL MATTERS

In so far as provision is made in relation to all the matters referred to in this Part, it is found in the DCC Licence and the provisions of the Code (including in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code).

9.1 FEES

See the statement at the beginning of this Part.

9.1.1 Certificate Issuance or Renewal Fees

See the statement at the beginning of this Part.

9.1.2 IKI Certificate Access Fees

See the statement at the beginning of this Part.

9.1.3 Revocation or Status Information Access Fees

See the statement at the beginning of this Part.

9.1.4 Fees for Other Services

See the statement at the beginning of this Part.

9.1.5 Refund Policy

See the statement at the beginning of this Part.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

See the statement at the beginning of this Part.

9.2.2 Other Assets

See the statement at the beginning of this Part.

9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

See the statement at the beginning of this Part.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.2 Information not within the Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.3 Responsibility to Protect Confidential Information

See the statement at the beginning of this Part.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

See the statement at the beginning of this Part.

9.4.2 Information Treated as Private

See the statement at the beginning of this Part.

9.4.3 Information not Deemed Private

See the statement at the beginning of this Part.

9.4.4 Responsibility to Protect Private Information

See the statement at the beginning of this Part.

9.4.5 Notice and Consent to Use Private Information

See the statement at the beginning of this Part.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

See the statement at the beginning of this Part.

9.4.7 Other Information Disclosure Circumstances

See the statement at the beginning of this Part.

9.5 INTELLECTUAL PROPERTY RIGHTS

See the statement at the beginning of this Part.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 Certification Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.2 Registration Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.3 Subscriber Representations and Warranties

See the statement at the beginning of this Part.

9.6.4 Relying Party Representations and Warranties

See the statement at the beginning of this Part.

9.6.5 Representations and Warranties of Other Participants

See the statement at the beginning of this Part.

9.7 DISCLAIMERS OF WARRANTIES

See the statement at the beginning of this Part.

9.8 LIMITATIONS OF LIABILITY

See the statement at the beginning of this Part.

9.9 INDEMNITIES

See the statement at the beginning of this Part.

9.10 TERM AND TERMINATION

9.10.1 Term

See the statement at the beginning of this Part.

9.10.2 Termination of IKI Certificate Policy

See the statement at the beginning of this Part.

9.10.3 Effect of Termination and Survival

See the statement at the beginning of this Part.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 Subscribers

See the statement at the beginning of this Part.

9.11.2 IKI Certification Authority

See the statement at the beginning of this Part.

9.11.3 Notification

See the statement at the beginning of this Part.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

See the statement at the beginning of this Part.

9.12.2 Notification Mechanism and Period

See the statement at the beginning of this Part.

9.12.3 Circumstances under which OID Must be Changed

See the statement at the beginning of this Part.

9.13 DISPUTE RESOLUTION PROVISIONS

See the statement at the beginning of this Part.

9.14 GOVERNING LAW

See the statement at the beginning of this Part.

9.15 COMPLIANCE WITH APPLICABLE LAW

See the statement at the beginning of this Part.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

See the statement at the beginning of this Part.

9.16.2 Assignment

See the statement at the beginning of this Part.

9.16.3 Severability

See the statement at the beginning of this Part.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

See the statement at the beginning of this Part.

9.16.5 Force Majeure

See the statement at the beginning of this Part.

9.17 OTHER PROVISIONS

9.17.1 IKI Certificate Policy Content

See the statement at the beginning of this Part.

9.17.2 Third Party Rights

See the statement at the beginning of this Part.

Annex A: Definitions and Interpretation

In this Policy, except where the context otherwise requires -

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section,
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below,
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy.

Activation Data	means any private Data (such as a password or the Data on a smartcard) which are used to access a Cryptographic Module.
Archive	means the archive of Data created in accordance with Part 5.5.1 of this Policy (and "**Archives**" and "**Archived**" shall be interpreted accordingly).
Audit Log	means the audit log created in accordance with Part 5.4.1 of this Policy.
Authentication	means the process of establishing that an individual, Certificate, System or Organisation is what he or it claims to be (and "**Authenticate**" shall be interpreted accordingly).
Authorised Responsible Officer (ARO)	means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, an RDP, a DCC Service Provider, the SMKI PMA or the Panel in accordance with the SMKI RAPP
Authorised Subscriber	means a Party or RDP which has successfully completed the procedures set out in this Policy and has been authorised by the ICA to submit a Certificate Signing Request.
Certificate	means either an IKI Certificate or an ICA Certificate.
Certificate Profile	means a table bearing that title in Annex B and specifying

	certain parameters to be contained within a Certificate.
Certificate Re-Key	means a change to the Public Key contained within a Certificate bearing a particular serial number.
Certificate Revocation Request	means a request for the revocation of a Certificate by the ICA, submitted by the Subscriber for that Certificate to the ICA in accordance with the SMKI RAPP and this Policy.
Certificate Signing Request	means a request for a Certificate submitted by an Eligible Subscriber in accordance with the SMKI RAPP.
Eligible Subscriber	means: a) in respect of each IKI Certificate Issued by the IKI Administrator CA or the IKI Registration Authority CA, the DCC; b) in respect of each IKI Certificate Issued by the IKI Authorised Organisation Subscriber CA, each Eligible Subscriber in respect of Organisation Certificates; c) in respect of each IKI Certificate Issued by the IKI Authorised Device Subscriber CA, each Eligible Subscriber in respect of Device Certificates; d) in respect of each IKI Certificate Issued by the IKI Authorised Web Service Subscriber CA, each Eligible Subscriber for Device Certificates that is the DCC or a Supplier; or e) in respect of each ICA Certificate, the DCC.
ICA	See IKI Certification Authority
ICA Certificate	means either a Root ICA Certificate or an Issuing ICA Certificate.
ICA Key	means any Private Key or a Public Key generated by the ICA for the purposes of complying with its obligations under the Code.
ICA Private Key	means either a Root ICA Private Key or an Issuing ICA Private

	Key.
ICA Systems	means the Systems used by the ICA in relation to the SMKI Services.
IKI Certification Authority (or ICA)	means the DCC, acting in the capacity and exercising the functions of one or more of: (a) the Root ICA; (b) the Issuing ICA; and (c) the Registration Authority.
IKI Administrator Certificate Authority (or CA)	Means an ICA Issuing Certificates to Registration Authority Personnel, Registration Authority Managers and Authorised Responsible Officers acting on behalf of DCC Service Providers for the purposes of authenticating such persons to SMKI Services
IKI Authorised Device Subscriber Certificate Authority (or CA)	Means an ICA Issuing Certificates for the purposes of authenticating Authorised Responsible Officers to SMKI Services for the purposes of submitting CSRs in respect of Device Certificates
IKI Authorised Organisation Subscriber Certificate Authority (or CA)	Means an ICA Issuing Certificates for the purposes of authenticating Authorised Responsible Officers to SMKI Services for the purposes of submitting CSRs and CRRs in respect of Organisation Certificates
IKI Authorised Web Service Subscriber Certificate Authority (or CA)	Means an ICA Issuing Certificates to Authorised Subscribers for the purposes of authenticating a Subscriber's Systems to SMKI Services for the purposes of submission of CSRs in respect of Device Certificates via the Web Service interface
IKI Authority Revocation List (or IKI ARL)	means a list, produced by the ICA, of all ICA Certificates that have been revoked in accordance with this Policy.
IKI Certificate	means a certificate in the form set out in the IKI Certificate Profile in accordance with Annex B, and Issued by the Issuing

	ICA in accordance with this Policy
IKI Registration Authority Certificate Authority (or CA)	Means an ICA Issuing Certificates to DCC Systems for the purposes of authenticating such Systems to SMKI Services
Issue	means the act of the ICA, in its capacity as the Root ICA or Issuing ICA, and acting in accordance with this Policy, of creating and signing a Certificate which is bound to both a Subject and a Subscriber (and "Issued" and "Issuing" shall be interpreted accordingly).
Issuing ICA Certificate	means a certificate in the form set out in the Issuing ICA Certificate Profile in accordance with Annex B, and Issued by the Root ICA to one of five Issuing ICAs in accordance with this Policy. The permitted Issuing ICAs are: a) IKI Administrator CA; b) IKI Registration Authority CA; c) IKI Authorised Organisation Subscriber CA; d) IKI Authorised Device Subscriber CA; and e) IKI Authorised Web Service Subscriber CA.
Issuing ICA Private Key	means a Private Key which is stored and managed by the ICA acting in its capacity as the Issuing ICA.
Issuing ICA Public Key	means the Public Key which is part of a Key Pair with an Issuing ICA Private Key.
Issuing IKI Certification Authority (or Issuing ICA)	means the DCC exercising the function of Issuing IKI Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function.
Key Escrow	means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.
Object Identifier (or OID)	means an Object Identifier assigned by the Internet Address Naming Authority.

Private Key Material	in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.
Registration Authority	means the DCC exercising the function of receiving and processing Certificate Signing Requests made in accordance with the SMKI RAPP.
Registration Authority Manager	means either a director of the DCC or any other person who may be identified as such in accordance with the SMKI RAPP.
Registration Authority Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the Registration Authority.
Relying Party	means a person who, pursuant to the Code, receives and relies upon a Certificate.
Root ICA Private Key	means a Private Key which is stored and managed by the ICA acting in its capacity as the Root ICA.
Root ICA Certificate	means a certificate in the form set out in the Root ICA Certificate Profile in accordance with Annex B and self-signed by the Root ICA in accordance with this Policy.
Root IKI Certification Authority (or Root ICA)	means the DCC exercising the function of Issuing ICA Certificates to the Issuing ICA and storing and managing Private Keys associated with that function.
Security Related Functionality	means the functionality of the ICA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of that System.
Subject	means: in relation to an IKI Certificate, the Entity identified in the 'Subject Name' field of the IKI Certificate Profile in Annex B; and in relation to an ICA Certificate, the globally unique name of the Root ICA or Issuing ICA as identified in the Subject field of the relevant Certificate Profile in Annex B.
Subscriber	means, in relation to any Certificate, a Party or RDP which has been Issued with and accepted that Certificate, acting in its

capacity as the holder of the Certificate.

Time-Stamping means the act that takes place when a Time-Stamping Authority, in relation to a Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.

Time-Stamping Authority means that part of the ICA that:

(a) where required, provides an appropriately precise time-stamp in the format required by this Policy; and

(b) relies on a time source that is:

(i) accurate;

(ii) determined in a manner that is independent of any other part of the ICA Systems; and

(iii) such that the time of any time-stamp can be verified to be that of the Independent Time Source at the time at which the time-stamp was applied.

Validity Period means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

Annex B: ICA Certificate and IKI Certificate Profiles

Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which ICA Certificates and IKI Certificates Certificates shall comply. All terms in this Annex shall, where not defined in the Code, this Policy, or the GB Companion Specification, have the meanings in IETF RFC5280.

Common requirements applicable to Root ICA Certificates, Issuing ICA Certificates and IKI Certificates

All ICA Certificates and IKI Certificates that are validly authorised within the SMKI for use within the scope of GB Smart Metering:

- shall be compliant with IETF RFC5280.
- all ICA Certificates and IKI Certificates shall:
    - contain the authorityKeyIdentifier extension, except where the Certificate is the Root ICA Certificate;
    - contain the keyUsage extension which shall be marked as critical;
- be X.509 v3 certificates as defined in IETF RFC 5280, encoded using the ASN.1 Distinguished Encoding Rules;
- only contain Public Keys that are 4096-bit RSA for the Root ICA Certificate or 2048-bit RSA Public Keys for all subordinate certificates which shall include Issuing OCA Certificates;
- only provide for signature methods that are RSA with SHA 256
- contain a certificatePolicies extension containing at least one PolicyIdentifier which shall be marked as critical. For clarity and in adherence with IETF RFC 5280, Certification Path Validation undertaken by Parties shall interpret this extension;
- contain a serialNumber of no more than 16 octets in length;
- contain a subjectKeyIdentifier which shall be marked as non-critical;
- contain an authorityKeyIdentifier in the form *option [0]* KeyIdentifier which shall be marked as non-critical, except where the Certificate is the Root ICA Certificate. Note this exception only applies where RemotePartyRole as specified in the X520OrganizationalUnitName field = root;
- only contain KeyIdentifiers generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280;
- contain an IssuerName which MUST be identical to the signer's SubjectName; and

- have a valid notBefore field consisting of the time of issue encoded and a valid notAfter field expiration date as per IETF RFC 5280 Section 4.1.2.5.

Requirements applicable to IKI Certificates only

All IKI Certificates that are Issued by an Issuing ICA shall:

- contain a non-empty subject field which for:
  - IKI Certificates issued by the IKI Administrator CA, contains an organisationalName whose value will be set to that of the Authorised Subscriber, an OrganizationalUnitName whose value shall be set to the subject's role, a commonName whose value will be set to the individual subject's name and an emailAddress whose value will be set to the individual subject's email address;
  - IKI Certificates issued by the IKIRegistration Authority CA, contains an organisationalName whose value will be set to that of the Authorised Subscriber, two OrganizationalUnitNames whose values define the subject's role and a commonName whose value will be set to the system name;
  - IKI Certificates issued by the IKI Authorised Organisation Subscriber CA, contains an organisationalName whose value will be set to that of the Authorised Subscriber, an OrganizationalUnitName whose value shall be set to the RemotePartyRole that this Certificate allows the subject of the certificate to perform and a commonName whose value will be set to the ARO's name;
  - IKI Certificates issued by the IKI Authorised Device Subscriber CA, contains an organisationalName whose value will be set to that of the Authorised Subscriber, an OrganizationalUnitName whose value shall be set to the RemotePartyRole that this Certificate allows the subject of the certificate to perform and a commonName whose value will be set to the ARO's or system name
  - IKI Certificates issued by the IKI Authorised Web Service Subscriber CA, contains an organisationalName whose value will be set to that of the Authorised Subscriber, an OrganizationalUnitName whose value shall be set to the RemotePartyRole that this Certificate allows the subject of the certificate to perform and a commonName whose value will be set to the systems name.
  - .
- contain a single Public Key;
- contain a keyUsage extension marked as critical, with value of:
  - digitalSignature;
- Contain a extKeyUsage extenion marked critical, with a value of:

- ClientAuth.
- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID of this Policy under which the Certificate is Issued.

Requirements applicable ICA Certificates only

All ICA Certificates Issued by the Root ICA shall:

- be such that, per RFC5280, the IssuerName MUST be identical to the signer's SubjectName;
- have a globally unique SubjectName;
- contain a single public key;
- contain a keyUsage extension marked as critical and defined as:
  - keyCertSign; and
  - cRLSign;
- for Issuing ICA Certificates, contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID of this Policy under which the Certificate is Issued;
- for the Root ICA Certificate, contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for any Policy;
- for Issuing ICA Certificates, contain the basicConstraints extension, with values cA=True, and pathLen=0. This extension shall be marked as critical;
- for the Root ICA Certificate, contain the basicConstraints extension, with the value cA=True and pathLen absent (unlimited). This extension shall be marked as critical.

IKI Certificate Profile

Field Name	**RFC 5759/5280 Type**	**Value**	**Reference**
Version	Integer	V3	
serialNumber	Integer	Positive Integer of up to 16 Octets	
Signature	AlgorithmIdentifier	SHA256 With RSA encryption	
Issuer	Name	Globally unique name of Issuing ICA	

Authoritykeyidentifier	KeyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	
subjectKeyIdentifier	KeyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the Certificate	
notAfter	Time	Expiry time of the Certificate	
Subject	Name	Name of the Subject	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
Extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	2048 bit RSA and SHA256,	
signatureValue	BIT STRING	Subject IKI Certificate signature	

Interpretation

Version

The version of the X.509 IKI Certificate. Valid IKI Certificates shall identify themselves as version 3.

serialNumber

IKI Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the IKI Certificate, and shall be created by the Issuing ICA that signs the IKI Certificate. The serialNumber shall be unique in the scope of IKI Certificate signed by the Issuing I CA.

Signature

The identity of the signature algorithm used to sign the IKI Certificate. The field is identical to the value of the IKI Certificate 'signatureAlgorithm' field explained further under the next '**signatureAlgorithm**' heading below.

Issuer

The name of the signer of the IKI Certificate. This will be the gloablly unique name of the Issuing ICA.

authorityKeyIdentifier

To optimize building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all IKI Certificates. The IKI Certificate shall contain a authorityKeyIdentifier in the form *option [0]* KeyIdentifier.

subjectKeyIdentifier

The Subject Key Identifier extension shall be included and marked as non-critical in the IKI Certificate. The IKI Certificate shall contain a subjectKeyIdentifier with KeyIdentifier generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and which shall always be 8 octets in length.

validity

The time period over which the Issuing ICA expects the IKI Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time an IKI Certificate may be used. This shall be the time the IKI Certificate is created.

notAfter

The latest time an IKI Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN) with the value as defined earlier in Annex B to this IKI Certificate Profile.

subjectPublicKeyInfo

The IKI Certificate subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 5280.The object identifiers for the supported algorithms and the methods for encoding the Public Key materials (public key and parameters) are specified in RFC3279, RFC4055, and RFC4491.

The algorithm field shall use the following identifier:

```
rsaEncryption ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
```

The rsaEncryption OID is intended to be used in the algorithm field of a value of type AlgorithmIdentifier. The parameters field MUST have ASN.1 type NULL for this algorithm identifier.

The RSA public key MUST be encoded using the ASN.1 type RSAPublicKey:

```
RSAPublicKey ::= SEQUENCE {

          modulus            INTEGER,    -- n

          publicExponent     INTEGER  }  -- e
```

where modulus is the modulus n, and publicExponent is the public exponent e. The DER encoded RSAPublicKey is the value of the BIT STRING subjectPublicKey.

signatureAlgorithm

The signatureAlgorithm field shall indicate the Issuing ICA signature algorithm used to sign this IKI Certificate is as defined under the next '**Signature Method**' heading below.

signatureValue

The Issuing ICA's signature of the IKI Certificate is computed using the Issuing ICA's private RSA 2048-bit IKI Certificate signing key using the algorithm identified under the next '**Signature Method (RSA)**' heading below.

The IKI Certificates shall be signed by the Issuing ICA using the RSA algorithm identified under the next '**Signature Method (RSA)**' heading below. The structure for RSA signatures is as per RFC 5280.

extensions

IKI Certificates SHOULD contain the extensions described below. They SHOULD NOT contain any additional extensions:

- certificatePolicy: critical; OID as a policyIdentifier

- keyUsage: critical; digitalSignature.
- extKeyUsage: critical;clientAuth
- basicConstraints: critical; cA=false.
- authorityKeyIdentifier.
- subjectKeyIdentifier.
- cRLDistributionPoint: non-critical; URI string, which shall identify the URL of the IKI CRL within the SMKI Repository
- Private extensions used internally by the SMKI application with an extension OID of 2.16.840.1.113733.1.16.3, 2.16.840.1.113733.1.16.4, 2.16.840.1.113733.1.16.5 or 2.16.840.1.113733.1.16.11 where:
  - 2.16.840.1.113733.1.16.3 - Contains Cert Profile OID
  - 2.16.840.1.113733.1.16.4 - Contains Account ID
  - 2.16.840.1.113733.1.16.5 - Contains Base64 encoded URL for Symantec PKI Client web service.
  - 2.16.840.1.113733.1.6.11 - Containd Jurisdiction Hash of Symantec Master account

Cryptographic Primitives for Signature Method

Signature Method (RSA)

The RSA signature method is defined in NIST FIPS 186-4. When implementing RSA, the SHA-256 message digest algorithm choice is identified based on section 5 of SP 800-57part1.

The signature algorithm shall be SHA256-with-RSA Encryption as specified in RFC4055. The algorithm identifier is:

```
sha256WithRSAEncryption(11) ::= {iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
sha256WithRSAEncryption(11)}
```

SHA-256 hash algorithm

The hash algorithm used by the IKI Certificate shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Root ICA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	Positive Integer of up to 16 Octets	
Signature	AlgorithmIdentifier	SHA256 With RSA Encryption,.	

Issuer	Name	Globally unique name of Root ICA	
subjectKeyIdentifier	KeyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	
notBefore	Time	Creation time of the Certificate	
notAfter	Time	Expiry time of the Certificate	
Subject	Name	Globally unique name of Root ICA (same as Issuer name)	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
Extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	4096 bit RSA and SHA256	
signatureValue	BIT STRING	Subject Certificate signature	

These certificates are the root of trust for the IKI

Version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

serialNumber

Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the Certificate, and shall be created by the ICA Certificate that signs the Certificate (self-signed by

Root ICA). The serialNumber shall be unique in the scope of Certificates signed by the ICA Certificate.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Root CA Certificate's signatureAlgorithm field explained further under the next '**Signature Method'** heading below.

Issuer

The name of the signer of the Certificate. This will be the gloablly unique name of the Root ICA. This will be the same as the SubjectName as it is self-signed by the Root ICA.

subjectKeyIdentifier

The Root ICA credentials contain the subjectKeyIdentifier extension. Adding subjectKeyIdentifer facilitates certificate path building, which is necessary to validate credentials.

The Subject Key Identifier extension shall be included and marked as non-critical in the Certificate. The Certificate shall contain a subjectKeyIdentifier with KeyIdentifier generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280.

validity

The time period over which the issuer expects the Certificate to be valid for. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

notAfter

The latest time a Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

subject

This field must be populated with the globally unique name of the Root ICA.

subjectPublicKeyInfo

The Root ICA Certificate subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 5280, where the key size shall be 4096-bit RSA. The object identifiers for the supported algorithms and the methods for encoding the public key materials (public key and parameters) are specified in RFC3279-, -RFC4055-, and -RFC4491-

The algorithm field shall use the following identifier:

```
rsaEncryption ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
```

The rsaEncryption OID is intended to be used in the algorithm field of a value of type AlgorithmIdentifier. The parameters field MUST have ASN.1 type NULL for this algorithm identifier.

The RSA public key MUST be encoded using the ASN.1 type RSAPublicKey:

```
RSAPublicKey ::= SEQUENCE {
    modulus            INTEGER,    -- n
    publicExponent     INTEGER  }  -- e
```

where modulus is the modulus n, and publicExponent is the public exponent e. The DER encoded RSAPublicKey is the value of the BIT STRING subjectPublicKey.

signatureAlgorithm

The signatureAlgorithm field shall indicate the Root ICA signature algorithm used to sign this Certificate as defined in section under the next '**Signature Method**' heading below.

signatureValue

The Root ICA's signature of the Certificate is computed using the Root iCA's private RSA 4096-bit Certificate signing key using the algorithm identified under the next '**Signature Method (RSA)**' heading below.

The Root ICA Certificates shall be signed by the Root ICA using the RSA algorithm identified under the next '**Signature Method (RSA)**' heading below. The structure for RSA signatures is as per RFC 5280.

extensions

Certificates MUST contain the extensions described below and MUST have the name form as described. They SHOULD NOT contain any additional extensions:

Extensions

- certificatePolicy: critical; OID as a policyIdentifier
- keyUsage: critical; keyCertSign, crlSign
- basicConstraints: critical; cA=true, pathLen absent (unlimited)
- subjectKeyIdentifer: non-critical; Method 2

Cryptographic Primitives for Signature Method

Signature Method (RSA)

The RSA signature method is defined in NIST FIPS 186-4. When implementing RSA, the SHA-256 message digest algorithm choice is identified based on section 5 of SP 800-57part1.

The signature algorithm shall be SHA256-with-RSA Encryption as specified in RFC4055. The algorithm identifier is:

```
sha256WithRSAEncryption(11) ::= {iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
sha256WithRSAEncryption(11)}
```

SHA-256 hash algorithm

The hash algorithm used by the Certificate shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Issuing ICA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	Positive Integer of up to 16 Octets	
Signature	AlgorithmIdentifier	SHA256 With RSA Encryption.	
Issuer	Name	Globally unique name of Root ICA	
subjectKeyIdentifier	KeyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	
authorityKeyIdentifier	KeyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	
notBefore	Time	Creation time of the certificate	
notAfter	Time	Expiry time of the Certificate	
Subject	Name	Globally unique name of Issuing ICA	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
Extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	2048-bit RSA and	

		SHA256	
signatureValue	BIT STRING	Subject certificate signature	

Version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

serialNumber

Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the Certificate, and shall be created by the Root ICA that signs the Certificate. The serialNumber shall be unique in the scope of Certificates signed by the Root ICA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing ICA Certificate's signatureAlgorithm field explained further under the next '**signatureAlgorithm**' heading below.

issuer

The name of the signer of the Certificate. This will be the gloablly unique name of the Root ICA.

subjectKeyIdentifier

The Issued credentials contain the subjectKeyIdentifier extension. Adding subjectKeyIdentifer facilitates certificate path building, which is necessary to validate credentials.

The Subject Key Identifier extension shall be included and marked as non-critical in the Certificate. The Certificate shall contain a subjectKeyIdentifier with KeyIdentifier generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and which shall always be 8 octets in length.

authorityKeyIdentifier

To optimize building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all IKI Certificates. The Certificates shall contain a authorityKeyIdentifier in the form *option [0]* KeyIdentifier.

validity

The time period over which the issuer expects the Certificate to be valid for. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

notAfter

The latest time a Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

subject

This field must be populated with the globally unique name of the Issuing ICA.

subjectPublicKeyInfo (RSA)

The Issuing ICA Certificate subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 5280, where the key size shall be 2048-bit RSA. The object identifiers for the supported algorithms and the methods for encoding the public key materials (public key and parameters) are specified in RFC3279, RFC4055, and RFC4491.

The algorithm field shall use the following identifier:

```
rsaEncryption ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
```

The rsaEncryption OID is intended to be used in the algorithm field of a value of type AlgorithmIdentifier. The parameters field MUST have ASN.1 type NULL for this algorithm identifier.

The RSA public key MUST be encoded using the ASN.1 type RSAPublicKey:

```
RSAPublicKey ::= SEQUENCE {
   modulus            INTEGER,    -- n
   publicExponent     INTEGER  }  -- e
```

where modulus is the modulus n, and publicExponent is the public exponent e. The DER encoded RSAPublicKey is the value of the BIT STRING subjectPublicKey.

signatureAlgorithm

The signatureAlgorithm field shall indicate the Root ICA signature algorithm used to sign this Certificate as defined under the next '**Signature Method**' heading below.

signatureValue

The Root ICA's signature of the Certificate is computed using the Root ICA's private RSA 4096-bit private signing key using the algorithm identified under the next '**Signature Method (RSA)**' heading below.

The Certificates shall be signed by the Root ICA using the RSA algorithm identified under the next '**Signature Method (RSA)**' heading below. The structure for RSA signatures is as per RFC 5280.

extensions

Issuing ICA certificates MUST contain the extensions described below and MUST have the name form as described. They SHOULD NOT contain any additional extensions:

- certificatePolicy: critical; OID as a policyIdentifier
- keyUsage: critical; keyCertSign, crlSign
- basicConstraints: critical; cA=true, pathLen=0
- subjectKeyIdentifer: non-critical; Method 2
- authorityKeyIdentifier: non-critical; Option [0]
- subjectAltName: non-critical; pointer in the form of an X500 directory name for the associated Private Key on the relevant Cryptographic Module in which the Private Key is stored.
- cRLDistributionPoint: non-critical; URI string

Cryptographic Primitives for Signature Method

Signature Method (RSA)

The RSA signature method is defined in NIST FIPS 186-4. When implementing RSA, the SHA-256 message digest algorithm choice is identified based on section 5 of SP 800-57 part1.

The signature algorithm shall be SHA256-with-RSA Encryption as specified in RFC4055. The algorithm identifier is:

```
sha256WithRSAEncryption(11) ::= {iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
sha256WithRSAEncryption(11)}
```

SHA-256 hash algorithm

The hash algorithm used by the Certificate shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.