**Version A4.0**

# Appendix A

# Device Certificate Policy

# CONTENTS

# 1 INTRODUCTION

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

- shall be known as the " **Device Certificate Policy**" (and in this document is referred to simply as the "**Policy**"),
- 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) Device Certificates; and

(ii) DCA Certificates.

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

(C) Except where the context otherwise requires, words or expressions used in this Policy shall have the meanings ascribed to them in IETF RFC 5280 where they:

(i) appear in `Courier New` font;

(ii) are accompanied by the descriptor 'field', 'type' or 'extension'; and/or

(iii) take the form of a conjoined string of two or more words, such as '`digitalSignature`'.

## 1.2 DOCUMENT NAME AND IDENTIFICATION

(A) This Policy has been assigned an OID of 1.2.826.0.1. 8641679.1.2.1.2.

## 1.3 SMKI PARTICIPANTS

### 1.3.1 The Device Certification Authority

(A) The definition of Device 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 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;

(ii) Eligible Subscriber;

(iii) Subscriber.

### 1.3.4 Subjects

(A) The Subject of a Device Certificate must be a Device (other than a Type 2 Device) represented by the identifier in the `subjectAltName` field of the Device Certificate Profile in accordance with Annex B.

(B) The Subject of a DCA Certificate must be the entity identified by the

`subject` field of the Root DCA Certificate Profile or Issuing DCA 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.

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

### 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 DEVICE CERTIFICATES AND DCA CERTIFICATES

### 1.4.1 Appropriate Certificate Uses

(A) The DCA shall ensure that Device Certificates are Issued only:

(i) subject to paragraph (B), to Eligible Subscribers; and

(ii) for the purposes of the creation, sending, receipt and processing of communications to and from Devices in accordance with or pursuant to the Code.

(B) For the purposes of paragraph (A), the DCA may treat any of the following as if they were an Eligible Subscriber:

(i) in relation to a Device that has an SMI Status that is not set to 'commissioned' or 'installed not commissioned', any Authorised Subscriber; or

(ii) in relation to a Device that has an SMI Status of 'commissioned' or 'installed not commissioned', the DCC or any Authorised Subscriber that is a User which acts (or is to act) in the User Role of either Import Supplier or Gas Supplier.

(C) The DCA shall ensure that DCA Certificates are Issued only to the DCA:

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

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

(D) 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 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 DCA or the SMKI PMA.

### 1.5.3 Person Determining Device CPS Suitability for the Policy

(A) Provision is made in Section L9.8 (d) of the Code for the SMKI PMA to approve the Device CPS.

### 1.5.4 Device CPS Approval Procedures

(A) Provision is made in Section L9.9 of the Code for the procedure by which the SMKI PMA may approve the Device 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

(A) 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 DCA shall lodge copies of the following in the SMKI Repository:

(i) each Device Certificate that has been accepted by a Subscriber;

(ii) each DCA Certificate;

(iii) each version of the SMKI RAPP;

(iv) each version of the SMKI Recovery Procedure; 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 DCA 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 DCA shall ensure that:

(i) each Device Certificate is lodged in the SMKI Repository promptly on its acceptance by a Subscriber;

(ii) each DCA Certificate is lodged to the SMKI Repository promptly on being Issued;

(iii) the Policy is lodged in the SMKI Repository, and a revised version of

the Policy is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(iv) 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;

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

(vi) 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 Sections L5.5, L5.6 and L5.6A of the Code.

# 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 Subject of each Certificate 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 Certificate 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 Eligible Subscribers from requesting the Issue of a Certificate anonymously or by means of a pseudonym; and

(ii) permit the DCA to Authenticate each Eligible Subscriber.

### 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 Eligible Subscriber in order to prove its possession of the Private Key which is associated with the Public Key to be 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.

### 3.2.2 Authentication of Organisation Identity

(A) Provision is made in the SMKI RAPP section 5.5 in relation to the:

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

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

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

(B) Provision is made in the SMKI RAPP section 5 for the purpose of ensuring that the criteria in accordance with which the DCA shall Authenticate a Party shall be set to the level pursuant to the SMKI PMA Guidance on "Verifying Organisation Identity" published on the Website.

### 3.2.3 Authentication of Individual Identity

(A) Provision is made in the SMKI RAPP sections 5.2 and 5.3 in relation to the Authentication of persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.

### 3.2.4 Authentication of Devices

(A) Not used.

### 3.2.5 Non-verified Subscriber Information

(A) The DCA shall:

(i) verify all information in relation to DCA Certificates;

(ii) require each Eligible Subscriber to verify the information contained in any Certificate Signing Request in respect of a Device Certificate.

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

### 3.2.6 Validation of Authority

See Part 3.2.2 of this Policy.

### 3.2.7 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 DCA 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

[*Not applicable in this Policy*]

# 4 CERTIFICATE LIFE-CYCLE 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 a Device Certificate:

(a) the circumstances in which an Eligible Subscriber 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 where applicable in the SMKI RAPP sections 5 and 6 in relation to the:

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

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

### 4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP section 6 in relation to the establishment of an enrolment process in respect of DCA Personnel and DCA Systems:

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

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

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

(b) for all SMKI Registration Authority Personnel to have their identify and authorisation verified to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.

## 4.2 CERTIFICATE APPLICATION PROCESSING

### 4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the SMKI RAPP section 5 in relation to the Authentication by the DCA of 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, the SMKI Interface Design Specification (SMKI IDS), this Policy or any other provision of the Code, the DCA:

(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 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, SMKI IDS, this Policy or any other provision of the Code, the DCA shall Issue the Certificate which was the subject of the Certificate Signing Request.

### 4.2.3 Time to Process Certificate Applications

(A) Provision in relation to the performance of the SMKI Services by the DCA is made in Section L8 of the Code (SMKI Performance Standards and

Demand Management).

## 4.3 CERTIFICATE ISSUANCE

### 4.3.1 DCA Actions during Certificate Issuance

(A) The DCA may Issue a Certificate only:

(i) in accordance with the provisions of this Policy, the SMKI RAPP and the SMKI IDS; and

(ii) in response to a Certificate Signing Request made by an Eligible Subscriber in accordance with the SMKI RAPP.

(B) The DCA shall ensure that:

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

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

(C) A DCA Certificate may only be:

(i) Issued by the DCA; and

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

(D) A Device Certificate may only be:

(i) Issued by the DCA; and

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

(E) The DCA shall not Issue a Device Certificate which is signed using an Issuing DCA Private Key after the first in time of the following:

(i) the time which is three months after the time at which any element of the Issuing DCA Private Key first became operational;

(ii) the time at which the DCA Issues the 100,000$^{th}$ Device Certificate

which is signed using that Issuing DCA Private Key.

(F) For the purposes of paragraph (E), the DCA shall ensure that the Device CPS incorporates:

(i) a procedure for determining:

(a) how the DCA will calculate when each of the times specified in that paragraph occurs; and

(b) for that purpose, when any element of the Issuing DCA Private Key first became operational; and

(ii) provisions for notifying the SMKI PMA when either of the times specified in that paragraph is approaching.

(G) The DCA shall not issue a Certificate containing a Public Key where it is aware that the Public Key is the same as the Public Key contained in any other Certificate that was previously issued by it.

### 4.3.2 Notification to Eligible Subscriber by the DCA of Issuance of Certificate

(A) Provision is made in the SMKI IDS sections 2.3.1.9, 2.4.1.4 and 2.5.1.4for the DCA to notify an Eligible Subscriber where that Eligible Subscriber is Issued with a Certificate which was the subject of a Certificate Signing Request made by it.

## 4.4 CERTIFICATE ACCEPTANCE

### 4.4.1 Conduct Constituting Certificate Acceptance

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

(i) specify a means by which an Eligible Subscriber may clearly indicate to the DCA its rejection of a Certificate which has been Issued to it (SMKI IDS sections 2.3.1.10, 2.4.1.5 and 2.5.1.5); and

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

Certificate (SMKI IDS section 2.2).

(B) A Certificate which has been Issued by the DCA 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 DCA 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 L11.6 of the Code.

### 4.4.2 Publication of Certificates by the DCA

(A) Provision in relation to the publication of Certificates is made in Part 2 of this Policy.

### 4.4.3 Notification of Certificate Issuance by the DCA to Other Entities

(A) The DCA 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 (SMKI IDS sections 2.3.1.9, 2.4.1.4 and 2.5.1.4).

## 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 L11.8 of the Code; 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 DCA may only replace, and shall not renew, any Certificate.

### 4.6.2 Circumstances of Certificate Replacement

(A) Where the DCA Systems or any DCA Private Key is (or is suspected by the DCA of being) Compromised, the DCA 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 a DCA Private Key:

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

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

(c) promptly both notify the SMKI PMA and verifiably destroy the DCA Private Key Material.

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

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

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

(C) An Eligible Subscriber may request a replacement for a Certificate at any time by applying for the Issue of a new Device Certificate in accordance with

this Policy.

**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 DCA**

See Part 4.4.2 of this Policy.

**4.6.8 Notification of Certificate Issuance by the DCA to Other Entities**

See Part 4.4.3 of 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 DCA shall not provide a Certificate Re-Key service.

(C) Where a new Key Pair has been generated by a Device, the Eligible Subscriber which is responsible for that Device shall apply for the Issue of a new Certificate in accordance with this Policy.

**4.7.2 Who may Request Certification of a New Public Key**

[*Not applicable in this Policy*]

### 4.7.3 Processing Certificate Re-Keying Requests

[*Not applicable in this Policy*]

### 4.7.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

### 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[*Not applicable in this Policy*]

### 4.7.6 Publication of the Re-Keyed Certificate by the DCA

[*Not applicable in this Policy*]

### 4.7.7 Notification of Certificate Issuance by the DCA to Other Entities

[*Not applicable in this Policy*]

## 4.8 CERTIFICATE MODIFICATION

### 4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification.

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

### 4.8.2 Who may request Certificate Modification

[*Not applicable in this Policy*]

### 4.8.3 Processing Certificate Modification Requests

[*Not applicable in this Policy*]

### 4.8.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

[*Not applicable in this Policy*]

### 4.8.6 Publication of the Modified Certificate by the DCA

[*Not applicable in this Policy*]

### 4.8.7 Notification of Certificate Issuance by the DCA to Other Entities

[*Not applicable in this Policy*]

## 4.9 CERTIFICATE REVOCATION AND SUSPENSION

### 4.9.1 Circumstances for Revocation

(A) This Policy does not support the revocation or suspension of Certificates.

(B) The DCA shall not provide any service of revoking or suspending a Certificate.

### 4.9.2 Who can Request Revocation

[*Not applicable in this Policy*]

### 4.9.3 Procedure for Revocation Request

[*Not applicable in this Policy*]

### 4.9.4 Revocation Request Grace Period

[*Not applicable in this Policy*]

### 4.9.5 Time within which DCA must process the Revocation Request

[*Not applicable in this Policy*]

### 4.9.6 Revocation Checking Requirements for Relying Parties

[*Not applicable in this Policy*]

### 4.9.7 CRL Issuance Frequency (if applicable)

[*Not applicable in this Policy*]

### 4.9.8 Maximum Latency for CRLs (if applicable)

[*Not applicable in this Policy*]

### 4.9.9 On-line Revocation/Status Checking Availability

[*Not applicable in this Policy*]

### 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

[*Not applicable in this Policy*]

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

(B) The DCA shall ensure that:

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

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

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

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

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

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

(F) The DCA shall ensure that the DCA Systems are Separated from any OCA

Systems, save that any Systems used for the purposes of the Registration Authority functions of the DCA and OCA shall not require to be Separated.

### 5.1.2 Physical Access

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

### 5.1.4 Water Exposure

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

### 5.1.5 Fire Prevention and Protection

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the DCA

Systems are situated.

### 5.1.6 Media Storage

(A) The DCA shall ensure that the Device 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 DCA.

### 5.1.7 Waste Disposal

(A) The DCA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the DCA are disposed of only using secure methods of disposal in accordance with https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.

### 5.1.8 Off-Site Back-Up

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

(i) all Data held on the DCA 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 DCA shall ensure that the Device CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The DCA 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 Device CPS, including when being

transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise DCA 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 DCA shall ensure that, where any elements of the DCA Systems, any Data held for the purposes of providing the SMKI Services, or any items of DCA 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 DCA shall ensure that:

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

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

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

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

### 5.2.2 Number of Persons Required per Task

(A) The DCA shall ensure that the Device CPS incorporates provisions designed to establish:

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

(ii) the application of controls to the actions of all members of DCA Personnel who are Privileged Persons, identifying in particular any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions.

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

(i) DCA Systems administration;

(ii) DCA Systems operations;

(iii) DCA Systems security; and

(iv) DCA 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 DCA shall ensure that all DCA 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 DCA, not have been previously relieved of any past assignment (whether for the DCA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The DCA shall ensure that all DCA 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 DCA shall ensure that the Device CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of DCA Personnel.

**5.3.5 Job Rotation Frequency and Sequence**

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

**5.3.6 Sanctions for Unauthorised Actions**

(A) The DCA shall ensure that the Device CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by

members of DCA Personnel.

### 5.3.7 Independent Contractor Requirements

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

### 5.3.8 Documentation Supplied to Personnel

(A) The DCA shall ensure that all DCA 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 Device CPS; and

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

## 5.4 AUDIT LOGGING PROCEDURES

### 5.4.1 Types of Events Recorded

(A) The DCA shall ensure that:

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

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

(a) the activities of DCA Personnel;

(b) the use of DCA equipment;

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

(d) communications and activities that are related to the Issue of

Certificates (in so far as not captured by the DCA 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 DCA shall ensure that:

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

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

(a) British Standard BS 10008:2014 (Evidential Weight and Legal Admissibility of Electronic Information); or

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

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

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

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

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

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

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

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

### 5.4.3 Retention Period for Audit Log

(A) The DCA 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 DCA 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 10008:2014 (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 DCA 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 DCA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The DCA 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 Device 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 DCA shall ensure that the Device 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 DCA shall ensure that the Device 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 DCA Systems.

**5.5 RECORDS ARCHIVAL**

**5.5.1 Types of Records Archived**

(A) The DCA 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 DCA 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 DCA 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 DCA shall ensure that the Device 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 DCA shall ensure that the Device 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 DCA 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 DCA's operations.

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

## 5.6 KEY CHANGEOVER

### 5.6.1 Device Certificate Key Changeover

(A) The DCA shall Issue a new Device Certificate in relation to a Device where a new Certificate Signing Request is submitted by an Eligible Subscriber in accordance with the requirements of the SMKI IDS sections 2.3.1.6 to 2.3.1.10, 2.4.1.1 to 2.4.1.5 and 2.5.1.1 to 2.5.1.4and this Policy.

### 5.6.2 DCA Key Changeover

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

(i) verifiably destroy the Issuing DCA Private Key Material;

(ii) not revoke the related Issuing DCA Certificate (which may continue to be used for the purpose of validating Digital Signatures generated using the Issuing DCA Private Key);

(iii) generate a new Key Pair;

(iv) ensure that any Device Certificate subsequently Issued by it is Issued using the Issuing DCA 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

(v) in its capacity as the Root DCA:

(a) Issue a new Issuing DCA Certificate; and

(b) promptly lodge that Issuing DCA Certificate in the SMKI Repository.

(B) The DCA 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.

## 5.7 COMPROMISE AND DISASTER RECOVERY

### 5.7.1 Incident and Compromise Handling Procedures

(A) The DCA shall ensure that the Device CPS incorporates a business continuity plan which shall be designed to ensure 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 DCA Systems or major failure in the DCA processes.

(B) The DCA 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) In the event of the Compromise of any DCA Private Key, the DCA shall:

(i) not revoke the related Issuing DCA Certificate;

(ii) not revoke any Device Certificates Issued using the Issuing DCA Private Key;

(iii) not issue any further Device Certificates using the Issuing DCA Private Key;

(iv) treat the event in the same manner as if it were a Major Security Incident in accordance with Section G2 of the Code (System Security: Obligations on the DCC); and

(v) immediately notify the SMKI PMA.

(D) The DCA shall ensure that the Device 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 Issuing DCA Private Key or any part of the DCA Systems is Compromised.

**5.7.2 Computing Resources, Software and/or Data are Corrupted**

(A) The DCA 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 DCA 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 DCA shall ensure that the Device 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 DCA, the Issuing DCA and the Registration Authority.

## 6.1 KEY PAIR GENERATION AND INSTALLATION

### 6.1.1 Key Pair Generation

(A) The DCA shall ensure that all Key Pairs which it uses for the purposes of this Policy 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 DCA Key; and

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

(B) The DCA shall not generate any Private Key or Public Key other than a DCA Key.

### 6.1.2 Private Key Delivery to Subscriber

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

### 6.1.3 Public Key Delivery to Certificate Issuer

(A) The DCA shall ensure that the Device 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 DCA and Issuing DCA; and

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

### 6.1.4 DCA Public Key Delivery to Relying Parties

(A) The DCA shall ensure that the Device CPS incorporates provisions:

(i) in relation to the manner by which each DCA Public Key is to be lodged in the SMKI Repository; and

(ii) designed to ensure that the DCA Public Keys are securely lodged in the SMKI Repository in such a manner as to guarantee that their integrity is maintained.

### 6.1.5 Key Sizes

(A) The DCA 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 size and characteristics set out in the GB Companion Specification.

### 6.1.6 Public Key Parameters Generation and Quality Checking

(A) The DCA 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 `keyUsage` Field)

(A) The DCA shall ensure that each Certificate that is Issued by it has a `keyUsage` field in accordance with RFC5759 and RFC5280.

(B) The DCA shall ensure that each Device Certificate that is Issued by it has a `keyUsage` of either:

(i) `digitalSignature`; or

(ii) `keyAgreement`.

(C) The DCA shall ensure that each DCA Certificate that is Issued by it has a `keyUsage` of `keyCertSign`.

(D) The DCA shall ensure that no `keyUsage` values may be set in a Device Certificate or DCA Certificate other than in accordance with this Part 6.1.7.

## 6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

### 6.2.1 Cryptographic Module Standards and Controls

(A) The DCA shall ensure that all DCA 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 DCA shall ensure that all DCA 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 DCA shall ensure that no DCA 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 DCA 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 Device CPS; and

(ii) be required to be unblocked by an authorised member of DCA Personnel who has been Authenticated as such following a process which shall be set out in the Device 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 DCA shall not provide any Key Escrow service.

### 6.2.4 Private Key Back-Up

(A) The DCA may Back-Up DCA 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 DCA Private Key in accordance with this Policy.

### 6.2.5 Private Key Archival

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

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The DCA shall ensure that no DCA 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 DCA shall ensure that the Cryptographic Module in which any DCA Private Key is stored may be accessed only by an authorised member of DCA 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 DCA shall ensure that any DCA Private Key shall be capable of being de-activated by means of the DCA 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 Device CPS.

### 6.2.10 Method of Destroying Private Key

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

(B) The DCA shall ensure that no DCA 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 DCA 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 DCA shall ensure that it archives DCA 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 DCA shall ensure that:

(i) the Validity Period of each Certificate shall be an indefinite period; and

(ii) for this purpose, it uses the `notAfter` value specified in Annex B.

## 6.4 ACTIVATION DATA

### 6.4.1 Activation Data Generation and Installation

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

(B) The DCA 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 DCA Keys; and

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

**6.4.2 Activation Data Protection**

(A) The DCA shall ensure that the Device 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 DCA shall ensure that the Device 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 DCA;

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

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

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

(v) the audit of security related events; and

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

### 6.5.2 Computer Security Rating

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

## 6.6 LIFE-CYCLE TECHNICAL CONTROLS

### 6.6.1 System Development Controls

(A) The DCA shall ensure that any software which is developed for the purpose of establishing a functionality of the DCA 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 DCA shall ensure that the Device CPS incorporates provisions which are designed to ensure that the DCA 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 DCA

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

### 6.7.2 Protection Against Attack

(A) The DCA shall use its best endeavours to ensure that the DCA 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 DCA shall take reasonable steps to ensure that the DCA 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 DCA

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

### 6.7.4 Health Check of DCA Systems

(A) The DCA shall ensure that, in relation to the DCA Systems, a vulnerability assessment in accordance with Sections G2.13 – G2.15 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 DCA shall ensure that Time-Stamping takes place in relation to all Certificates and all other DCA activities which require an accurate record of time.

(B) The DCA shall ensure that the Device CA 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 DCA.

# 7 CERTIFICATE, CRL AND OCSP PROFILES

## 7.1 CERTIFICATE PROFILES

(A) The DCA 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)

[*Not applicable in this Policy*]

### 7.2.2 CRL and CRL Entry Extensions

[*Not applicable in this Policy*]

## 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

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

### 8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

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

### 8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

### 8.4 TOPICS COVERED BY ASSESSMENT

(A) 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

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

### 8.6 COMMUNICATION OF RESULTS

(A) 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

(A) See the statement at the beginning of this Part.

### 9.1.1 Certificate Issuance or Renewal Fees

(A) See the statement at the beginning of this Part.

### 9.1.2 Device Certificate Access Fees

(A) See the statement at the beginning of this Part.

### 9.1.3 Revocation or Status Information Access Fees

(A) See the statement at the beginning of this Part.

### 9.1.4 Fees for Other Services

(A) See the statement at the beginning of this Part.

### 9.1.5 Refund Policy

(A) See the statement at the beginning of this Part.

## 9.2 FINANCIAL RESPONSIBILITY

### 9.2.1 Insurance Coverage

(A) See the statement at the beginning of this Part.

### 9.2.2 Other Assets

(A) See the statement at the beginning of this Part.

### 9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

(A) See the statement at the beginning of this Part.

## 9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

### 9.3.1 Scope of Confidential Information

(A) See the statement at the beginning of this Part.

### 9.3.2 Information not within the Scope of Confidential Information

(A) See the statement at the beginning of this Part.

### 9.3.3 Responsibility to Protect Confidential Information

(A) See the statement at the beginning of this Part.

## 9.4 PRIVACY OF PERSONAL INFORMATION

### 9.4.1 Privacy Plan

(A) See the statement at the beginning of this Part.

### 9.4.2 Information Treated as Private

(A) See the statement at the beginning of this Part.

### 9.4.3 Information not Deemed Private

(A) See the statement at the beginning of this Part.

### 9.4.4 Responsibility to Protect Private Information

(A) See the statement at the beginning of this Part.

### 9.4.5 Notice and Consent to Use Private Information

(A) See the statement at the beginning of this Part.

### 9.4.6 Disclosure Pursuant to Judicial or Administrative Process

(A) See the statement at the beginning of this Part.

### 9.4.7 Other Information Disclosure Circumstances

(A) See the statement at the beginning of this Part.

## 9.5 INTELLECTUAL PROPERTY RIGHTS

(A) See the statement at the beginning of this Part.

## 9.6 REPRESENTATIONS AND WARRANTIES

### 9.6.1 Certification Authority Representations and Warranties

(A) See the statement at the beginning of this Part.

### 9.6.2 Registration Authority Representations and Warranties

(A) See the statement at the beginning of this Part.

### 9.6.3 Subscriber Representations and Warranties

(A) See the statement at the beginning of this Part.

### 9.6.4 Relying Party Representations and Warranties

(A) See the statement at the beginning of this Part.

### 9.6.5 Representations and Warranties of Other Participants

(A) See the statement at the beginning of this Part.

## 9.7 DISCLAIMERS OF WARRANTIES

(A) See the statement at the beginning of this Part.

## 9.8 LIMITATIONS OF LIABILITY

(A) See the statement at the beginning of this Part.

## 9.9 INDEMNITIES

(A) See the statement at the beginning of this Part.

## 9.10 TERM AND TERMINATION

### 9.10.1 Term

(A) See the statement at the beginning of this Part.

### 9.10.2 Termination of Device Certificate Policy

(A) See the statement at the beginning of this Part.

### 9.10.3 Effect of Termination and Survival

(A) See the statement at the beginning of this Part.

## 9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

### 9.11.1 Subscribers

(A) See the statement at the beginning of this Part.

### 9.11.2 Device Certification Authority

(A) See the statement at the beginning of this Part.

### 9.11.3 Notification

(A) See the statement at the beginning of this Part.

## 9.12 AMENDMENTS

### 9.12.1 Procedure for Amendment

(A) See the statement at the beginning of this Part.

### 9.12.2 Notification Mechanism and Period

(A) See the statement at the beginning of this Part.

### 9.12.3 Circumstances under which OID Must be Changed

(A) See the statement at the beginning of this Part.

## 9.13 DISPUTE RESOLUTION PROVISIONS

(A) See the statement at the beginning of this Part.

## 9.14 GOVERNING LAW

(A) See the statement at the beginning of this Part.

## 9.15 COMPLIANCE WITH APPLICABLE LAW

(A) See the statement at the beginning of this Part.

## 9.16 MISCELLANEOUS PROVISIONS

### 9.16.1 Entire Agreement

(A) See the statement at the beginning of this Part.

### 9.16.2 Assignment

(A) See the statement at the beginning of this Part.

### 9.16.3 Severability

(A) See the statement at the beginning of this Part.

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

(A) `See the statement at the beginning of this Part.

### 9.16.5 Force Majeure

(A) See the statement at the beginning of this Part.

## 9.17 OTHER PROVISIONS

### 9.17.1 Device Certificate Policy Content

(A) See the statement at the beginning of this Part.

### 9.17.2 Third Party Rights

(A) 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,
- the rule of interpretation set out at Part 1.1 of this Policy shall apply.

| | |
|---|---|
| **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, organisation, System or Device is what he or it claims to be (and "**Authenticate**" shall be interpreted accordingly). |
| **Authorised Subscriber** | means a Party or RDP which has successfully completed the procedures set out in the SMKI RAPP and has been authorised by the DCA to submit a Certificate Signing Request. |

| | |
|---|---|
| **Certificate** | means either a Device Certificate or a DCA 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 Signing Request** | means a request for a Certificate submitted by an Eligible Subscriber in accordance with the SMKI RAPP. |
| **DCA Key** | means any Private Key or a Public Key generated by the DCA for the purposes of complying with its obligations under the Code. |
| **DCA 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 DCA. |
| **DCA Private Key** | means a DCA Key which is a Private Key. |
| **DCA Public Key** | means a DCA Key which is a Public Key. |
| **DCA Systems** | means the Systems used by the DCA in relation to the SMKI Services. |
| **DCA Certificate** | means either a Root DCA Certificate or an Issuing DCA Certificate. |
| **Device Certificate** | means a certificate in the form set out in the Device Certificate Profile in accordance with Annex B, and Issued by the Issuing DCA in accordance with this Policy. |
| **Device Certification Authority** (or **DCA**) | means the DCC, acting in the capacity and exercising the functions of one or more of:<br>(a) the Root DCA; |

(b) the Issuing DCA; and

(c) the Registration Authority.

**Eligible Subscriber** means:

(a) in relation to a Device Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.16 of the Code (Device Certificates); and

(b) in relation to a DCA Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.17 of the Code (DCA Certificates).

**Issue** means the act of the DCA, in its capacity as the Root DCA or Issuing DCA, 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 Device Certification Authority** (or **Issuing DCA**) means the DCC exercising the function of Issuing Device Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function.

**Issuing DCA Certificate** means a certificate in the form set out in the Issuing DCA Certificate Profile in accordance with Annex B, and Issued by the Root DCA to the Issuing DCA in accordance with this Policy.

**Issuing DCA Private Key** means a Private Key which is stored and managed by the DCA acting in its capacity as the Issuing DCA.

**Issuing DCA Public Key** means the Public Key which is part of a Key Pair with an Issuing DCA Private Key.

| | |
|---|---|
| **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. |
| **OCA** | has the meaning given to that expression in Appendix B of the Code (Organisation Certificate Policy). |
| **OCA Systems** | has the meaning given to that expression in Appendix B of the Code (Organisation Certificate Policy). |
| **Policy** | means this Device Certificate Policy. |
| **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. |
| **Root Device Certification Authority** (or **Root DCA**) | means the DCC exercising the function of Issuing DCA Certificates to the Issuing DCA and storing and managing Private Keys associated with that function. |
| **Root DCA Certificate** | means a certificate in the form set out in the Root DCA Certificate Profile in accordance with Annex B and self-signed by the Root DCA in accordance with this Policy. |
| **Root DCA Private Key** | means a Private Key which is stored and managed by the DCA acting in its capacity as the Root DCA. |
| **Security Related Functionality** | means the functionality of the DCA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of that System. |

| | |
|---|---|
| **SMKI Registration Authority Manager** | has the meaning given to that expression in the SMKI RAPP. |
| **SMKI Registration Authority Personnel** | has the meaning given to that expression in the SMKI RAPP. |
| **Subject** | means:<br>(a) in relation to a Device Certificate, the Device identified by the Device ID in the `hwSerialNum` field of the Device Certificate Profile in Annex B; and<br>(b) in relation to a DCA Certificate, the Root DCA or Issuing DCA as identified by 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 DCA that:<br>(a) where required, provides an appropriately precise time-stamp in the format required by this Policy; and<br>(b) relies on a time source that is:<br>(i) accurate; |

(ii) determined in a manner that is independent of any other part of the DCA 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: DCA Certificate and Device Certificate Profiles

## End Entity Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which DCA Certificates and Device 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 RFC 5759 or IETF RFC 5280.

## Common requirements applicable to DCA Certificates and Device Certificates

All DCA Certificates and Device Certificates that are validly authorised within the SMKI for use within the scope of the GB Companion Specification:

- shall be compliant with IETF RFC 5759 and so with IETF RFC 5280.
- for clarity and in adherence with the requirements of IETF RFC 5759, all DCA Certificates and Device Certificates shall:
    - contain the `authorityKeyIdentifier` extension, except where the Certificate is the Root DCA 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 of types that are explicitly allowed by the GBCS. This means all Public Keys shall be elliptic curve Public Keys on the NIST P-256 curve;
- only contain Public Keys in uncompressed form i.e. contain an elliptic curve point in uncompressed form as detailed in Section 2.2 of IETF RFC 5480;
- only provide for signature methods that are explicitly allowed within the GBCS. This means using P-256 Private Keys with SHA 256 and ECDSA;
- contain a `certificatePolicies` extension containing at least one `CertPolicyID` which shall be marked as critical. For clarity and in adherence with IETF RFC 5280, Certification Path Validation undertaken by Devices 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 `[0] KeyIdentifier` which shall be marked as non-critical, except where the Certificate is the Root DCA Certificate;
- only contain `KeyIdentifiers` generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and so which shall always be 8 octets in length;
- contain an `issuer` field whose contents MUST be identical to the contents of the signer's `subject` field in the signer's Certificate;
- have a valid `notBefore` field consisting of the time of issue encoded and a valid `notAfter` field for a not well-defined expiraton date as per IETF RFC 5280 Section 4.1.2.5.

**Requirements applicable to Device Certificates only**

All Device Certificates that are issued by the DCA shall:

- not have a well-defined expiration date and so the `notAfter` shall be assigned the `GeneralizedTime` value of 99991231235959Z;
- have an empty `subject` field;
- contain `subjectAltName` extension which contains a single `GeneralName` of type `otherName` that is further sub-typed as a `hardwareModuleName` (id-on-`hardwareModuleName`) as defined in RFC 4108 section 5. The `hwSerialNum` field shall be set to the Device's Entity Identifier. In adherence to IETF RFC 5280, the `subjectAltName` shall be marked as critical;
- contain a single Public Key;
- contain a keyUsage extension marked as critical, with a value of only one of:
  - `digitalSignature`; or
  - `keyAgreement`.
- contain a single `CertPolicyID` in the `certificatePolicies` extension that refers to the OID applicable to the version of this Device Certificate Policy applicable at the time that the Device Certificate was issued.

**Requirements applicable to the Root DCA and Issuing DCA**

All DCA Certificates issued by the DCA shall:

- not have a well-defined expiration date and so the notAfter shall be assigned the `GeneralizedTime` value of 99991231235959Z;
- must have a Valid `notBefore` field consisting of the time of issue encoded as per RFC 5280;
- Per RFC 5280, the IssuerName of any certificates MUST be identical to the signer's `subject`;
- have a globally unique `subject`;
- contain a single Public Key;
- contain a `keyUsage` extension marked as critical and defined as `keyCertSign;`
- For Issuing DCA Certificates contain at least one `CertPolicyID` in the `certificatePolicies` extension that refers to the OID of the version of this Device Certificate Policy prevailing at the time.
- For the Root DCA Certificate contain a single `CertPolicyID` in the `certificatePolicies` extension that refers to the OID for `anyPolicy`.
- For Issuing DCA Certificates, contain the `basicConstraints` extension, with values `cA`=True, and `pathLen`=0. This extension shall be marked as critical.
- For the Root DCA Certificate, contain the `basicConstraints` extension, with the value `cA=True` and `pathLen absent` (unlimited). This extension shall be marked as critical.

**Device 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 ECDSA | |
| The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name") | UTF8String | Globally unique common name of Issuing DCA of up to 4 Octets (as defined in the Issuing DCA Certificate Profile) | |
| keyIdentifier in Authoritykeyidentifier (the "Authority Key Identifier") | keyIdentifier | A unique value that matches the subjectKeyIdentifier value of the issuer's credential | |
| keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier") | keyIdentifier | Provides a means for identifying certificates containing the particular Public Key used in an application | |
| notBefore | Time | Creation time of the Device Certificate | |
| notAfter | Time | shall be assigned the GeneralizedTime value of 99991231235959Z | |

| | | | |
|---|---|---|---|
| The `value` field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-commonName` (the "Subject X520 Common Name") | `UTF8String` | EMPTY | |
| `subjectAltName` | `OtherName` | contains a single `GeneralName` of type `OtherName` that is further sub-typed as a `HardwareModuleName` (`id-on-hardwareModuleName`) as defined in RFC 4108 section 5. The `hwSerialNum` field shall be set to the Device's Entity Identifier | |
| `subjectPublicKeyInfo` | `SubjectPublicKeyInfo` | The Subject's Public Key | |
| `extensions` | `Extensions` | Critical and non-critical extensions | |
| `signatureAlgorithm` | `AlgorithmIdentifier` | SHA256 with ECDSA | |
| `signatureValue` | `BIT STRING` | Subject Device Certificate signature | |

**Interpretation**

**`version`**

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

**`serialNumber`**

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

**`signature`**

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

**Issuer X520 Common Name**

The name of the signer of the Device Certificate. This will be the gloablly unique name of the Issuing DCA of up to 4 Octets (as defined in the Issuing DCA Certificate Profile).

**Authority Key Identifier**

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 Device Certificates.

**Subject Key Identifier**

The Subject Key Identifier extension should be included and marked as non-critical in the Device Certificate.

**validity**

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

Device Certificate are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Device Certificate are expected to accept this value indefinitely.

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 Device Certificate may be used. This shall be the time the Device Certificate is created.

**notAfter**

The latest time a Device Certificate is expected to be used. Device Certificate are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Device Certificate are expected to accept this value indefinitely.

**Subject X520 Common Name**

This field must be EMPTY.

**subjectAltName**

The non-critical subjectAltName extension shall contain a single GeneralName of type OtherName that is further sub-typed as a HardwareModuleName (id-on-hardwareModuleName) as defined in RFC 4108 section 5. The hwSerialNum field shall be set to the Device ID.

**subjectPublicKeyInfo**

The Device Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` Device Certificate extension (explained further under the next **`extensions`** heading below).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve         OBJECT IDENTIFIER
    -- implicitCurve   NULL
    -- specifiedCurve  SpecifiedECDomain
  }
```

Only the following field in ECParameters shall be used:

- `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The `OBJECT IDENTIFIER` for the curve choice to be used in Device Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

**`signatureAlgorithm`**

The `signatureAlgorithm` field shall indicate the Issuing DCA signature algorithm used to sign this Device Certificate is as defined under the next **Signature Method (ECDSA)** heading.

**`signatureValue`**

The Issuing DCA's signature of the Device Certificate shall be computed using the Issuing DCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

**`extensions`**

Device Certificates shall contain the extensions described below. They SHOULD NOT contain any additional `extensions`:

- `certificatePolicy`
- `subjectAltName`
- `keyUsage`
- `authorityKeyIdentifier`
- `subjectKeyIdentifier`

### Cryptographic Primitives for Signature Method

### Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }
```

### SHA-256 hash algorithm

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

### Root DCA 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 ECDSA | |
| The `value` field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-` | `UTF8String` | Globally unique common name of Root DCA of up to 4 Octets | |

| | | | |
|---|---|---|---|
| commonName (the "Issuer X520 Common Name") | | | |
| keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifider") | keyIdentifier | A unique value that matches the subjectKeyIdentifier of the issuer's credential | |
| notBefore | Time | Creation time of the Certificate | |
| notAfter | Time | shall be assigned the GeneralizedTime value of 99991231235959Z | |
| The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name") | UTF8String | Globally unique name of Root DCA of up to 4 Octets (same as Issuer name) | |
| subjectPublicKeyInfo | SubjectPublicKeyInfo | The Subject's Public Key | |
| extensions | Extensions | Critical and non-critical extensions | |

| | | | |
|---|---|---|---|
| signatureAlgorithm | AlgorithmIdentifier | SHA256 with ECDSA | |
| signatureValue | BIT STRING | Subject Certificate signature | |

These certificates are the root of trust for the Devices SMKI.

**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 DCA that signs the Certificate (self-signed by Root DCA). The serialNumber shall be unique in the scope of Certificates signed by the DCA.

**signature**

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

**Issuer X520 Common Name**

The name of the signer of the Certificate. This will be the gloablly unique name of the Root DCA of up to 4 Octets. This will be the same as the subject as it is self-signed by the Root DCA.

**Subject Key Identifier**

The subjectKeyIdentifier extension should be included and marked as non-critical in the Certificate.

**validity**

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

Root DCA certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Root DCA certificate are expected to accept this value indefinitely.

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. Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Certificate are expected to accept this value indefinitely.

**Subject X520 Common Name**

This field must be populated with the globally unique name of the Root DCA of up to 4 Octets.

**subjectPublicKeyInfo**

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall be use the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-
body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the Key Usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve         OBJECT IDENTIFIER
    -- implicitCurve   NULL
    -- specifiedCurve  SpecifiedECDomain
  }
```

Only the following field in ECParameters shall be used:

- `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an `OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in DCA Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

**`signatureAlgorithm`**

The `signatureAlgorithm` field shall indicate the Root DCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

**`signatureValue`**

The Root DCA's signature of the Certificate shall be computed using the Root DCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading .

The structure for ECDSA signatures shall be as per RFC 5480.

**`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`
- `keyUsage`
- `basicConstraints`
- `subjectKeyIdentifer`

**Cryptographic Primitives for Signature Method**

**Signature Method (ECDSA)**

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-
sha2(3) 2 }
```

**SHA-256 hash algorithm**

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

**Issuing DCA 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 ECDSA | |
| The value field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-commonName` (the "Issuer X520 Common Name") | `UTF8String` | Globally unique name of Root DCA of up to 4 Octets (as defined in the Root DCA Certificate Profile) | |
| `keyIdentifier` in `subjectKeyIdentifier` (the "Subject Key Identifier") | `keyIdentifier` | Provides a means for identifying certificates containing the particular Public Key used in an application | |

| | | | |
|---|---|---|---|
| keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier") | keyIdentifier | A unique value that matches the subjectKeyIdentifier value of the issuer's credential | |
| notBefore | Time | Creation time of the certificate | |
| notAfter | Time | shall be assigned the GeneralizedTime value of 99991231235959Z | |
| The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name") | UTF8String | Globally unique name of Issuing DCA of up to 4 Octets | |
| subjectPublicKeyInfo | SubjectPublicKeyInfo | The Subject's Public Key | |
| extensions | Extensions | Critical and non-critical extensions | |
| signatureAlgorithm | AlgorithmIdentifier | SHA256 with ECDSA | |
| 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 Issuing DCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Root DCA.

**`signature`**

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

**Issuer X520 Common Name**

The name of the signer of the Certificate. This will be the gloablly unique name of the Root DCA of up to 4 Octets (as defined in the Root DCA Certificate Profile).

**Subject Key Identifier**

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

**Authority Key Identifier**

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all device Certificates.

**`validity`**

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

Issuing DCA certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Issuing DCA certificate are expected to accept this value indefinitely.

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. Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Certificate are expected to accept this value indefinitely.

**Subject X520 Common Name**

This field shall be populated with the globally unique name of the Issuing DCA of up to 4 Octets.

**`subjectPublicKeyInfo`**

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
     namedCurve         OBJECT IDENTIFIER
     -- implicitCurve   NULL
     -- specifiedCurve  SpecifiedECDomain
   }
```

Only the following field in ECParameters shall be used:

- `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an `OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

**`signatureAlgorithm`**

The `signatureAlgorithm` field shall indicate the Root DCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

**`signatureValue`**

The Root DCA's signature of the Certificate shall be computed using the Root DCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

**`extensions`**

Issuing-CA certificates shall contain the `extensions` described below. They SHOULD NOT contain any additional extensions:

- `certificatePolicy`
- `keyUsage`
- `basicConstraints`
- `subjectKeyIdentifer`
- `authorityKeyIdentifier`
- `subjectAltName`

**Cryptographic Primitives for Signature Method**

**Signature Method (ECDSA)**

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-
sha2(3) 2 }
```

**SHA-256 hash algorithm**

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