Version B1.2 Draft

Appendix B

Organisation Certificate Policy

CONTENTS

Part Heading Page

1 INTRODUCTION 8
1.1 OVERVIEW 8
1.2 DOCUMENT NAME AND IDENTIFICATION 8
1.3 SMKI PARTICIPANTS 8
1.3.1 The Organisation Certification Authority 8
1.3.2 Registration Authorities 9
1.3.3 Subscribers 9
1.3.4 Subjects 9
1.3.5 Relying Parties 10
1.3.6 SMKI Policy Management Authority 10
1.3.7 SMKI Repository Provider 10
1.4 USAGE OF ORGANISATION CERTIFICATES AND OCA CERTIFICATES 10
1.4.1 Appropriate Certificate Uses 10
1.4.2 Prohibited Certificate Uses 11
1.5 POLICY ADMINISTRATION 11
1.5.1 Organisation Administering the Document 11
1.5.2 Contact Person 11
1.5.3 Person Determining Organisation CPS Suitability for the Policy 11
1.5.4 Organisation CPS Approval Procedures 11
1.5.5 Registration Authority Policies and Procedures 11
1.6 DEFINITIONS AND ACRONYMS 12
1.6.1 Definitions 12
1.6.2 Acronyms 12
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 13
2.1 REPOSITORIES 13
2.2 PUBLICATION OF CERTIFICATION INFORMATION 13
2.3 TIME OR FREQUENCY OF PUBLICATION 13
2.4 ACCESS CONTROLS ON REPOSITORIES 14
3 IDENTIFICATION AND AUTHENTICATION 15
3.1 NAMING 15
3.1.1 Types of Names 15
3.1.2 Need for Names to be Meaningful 15
3.1.3 Anonymity or Pseudonymity of Subscribers 15
3.1.4 Rules for Interpreting Various Name Forms 15
3.1.5 Uniqueness of Names 15
3.1.6 Recognition, Authentication, and Role of Trademarks 15
3.2 INITIAL IDENTITY VALIDATION 15
3.2.1 Method to Prove Possession of Private Key 16
3.2.2 Authentication of Organisation Identity 16
3.2.3 Authentication of Individual Identity 16
3.2.4 Non-verified Subscriber Information 17
3.2.5 Validation of Authority 17
3.2.6 Criteria for Interoperation 17
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 17
3.3.1 Identification and Authentication for Routine Re-Key 17
3.3.2 Identification and Authentication for Re-Key after Revocation 17
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 17
3.4.1 Authentication for Certificate Revocation Requests 17

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 19
4.1 CERTIFICATE APPLICATION 19
4.1.1 Submission of Certificate Applications 19
4.1.2 Enrolment Process and Responsibilities 19
4.1.3 Enrolment Process for the Registration Authority and its Representatives 19
4.2 CERTIFICATE APPLICATION PROCESSING 20
4.2.1 Performing Identification and Authentication Functions 20
4.2.2 Approval or Rejection of Certificate Applications 20
4.2.3 Time to Process Certificate Applications 20
4.3 CERTIFICATE ISSUANCE 21
4.3.1 OCA Actions during Certificate Issuance 21
(iii) Notification to Eligible Subscriber by the OCA of Issuance of Certificate 22
4.4 CERTIFICATE ACCEPTANCE 22
4.4.1 Conduct Constituting Certificate Acceptance 22
4.4.2 Publication of Certificates by the OCA 22
4.4.3 Notification of Certificate Issuance by the OCA to Other Entities 23
4.5 KEY PAIR AND CERTIFICATE USAGE 23
4.5.1 Subscriber Private Key and Certificate Usage 23
4.5.2 Relying Party Public Key and Certificate Usage 23
4.6 CERTIFICATE RENEWAL 23
4.6.1 Circumstances of Certificate Renewal 23
4.6.2 Circumstances of Certificate Replacement 23
4.6.3 Who May Request a Replacement Certificate 24
4.6.4 Processing Replacement Certificate Requests 24
4.6.5 Notification of Replacement Certificate Issuance to a Subscriber 24
4.6.6 Conduct Constituting Acceptance of a Replacement Certificate 25
4.6.7 Publication of a Replacement Certificate by the OCA 25
4.6.8 Notification of Certificate Issuance by the OCA to Other Entities 25
4.7 CERTIFICATE RE-KEY 25
4.7.1 Circumstances for Certificate Re-Key 25
4.7.2 Who may Request Certification of a New Public Key 25
4.7.3 Processing Certificate Re-Keying Requests 25
4.7.4 Notification of New Certificate Issuance to Subscriber 25
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 25
4.7.6 Publication of the Re-Keyed Certificate by the OCA 26
4.7.7 Notification of Certificate Issuance by the OCA to Other Entities 26
4.8 CERTIFICATE MODIFICATION 26
4.8.1 Circumstances for Certificate Modification 26
4.8.2 Who may request Certificate Modification 26
4.8.3 Processing Certificate Modification Requests 26
4.8.4 Notification of New Certificate Issuance to Subscriber 26
4.8.5 Conduct Constituting Acceptance of Modified Certificate 26
4.8.6 Publication of the Modified Certificate by the OCA 26
4.8.7 Notification of Certificate Issuance by the OCA to Other Entities 27
4.9 CERTIFICATE REVOCATION AND SUSPENSION 27
4.9.1 Circumstances for Revocation 27
4.9.2 Who can Request Revocation 28
4.9.3 Procedure for Revocation Request 28
4.9.4 Revocation Request Grace Period 29
4.9.5 Time within which OCA must process the Revocation Request 29
4.9.6 Revocation Checking Requirements for Relying Parties 29
4.9.7 CRL Issuance Frequency (if applicable) 29
4.9.8 Maximum Latency for CRLs (if applicable) 31

4.9.9 On-line Revocation/Status Checking Availability 31
4.9.10 On-line Revocation Checking Requirements 31
4.9.11 Other Forms of Revocation Advertisements Available 31
4.9.12 Special Requirements in the Event of Key Compromise 31
4.9.13 Circumstances for Suspension 31
4.9.14 Who can Request Suspension 31
4.9.15 Procedure for Suspension Request 31
4.9.16 Limits on Suspension Period 31
4.10 CERTIFICATE STATUS SERVICES 32
4.10.1 Operational Characteristics 32
4.10.2 Service Availability 32
4.10.3 Optional Features 32
4.11 END OF SUBSCRIPTION 32
4.12 KEY ESCROW AND RECOVERY 33
4.12.1 Key Escrow and Recovery Policies and Practices 33
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 33
5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS 34
5.1 PHYSICAL CONTROLS 34
5.1.1 Site Location and Construction 34
5.1.2 Physical Access 35
5.1.3 Power and Air Conditioning 35
5.1.4 Water Exposure 35
5.1.5 Fire Prevention and Protection 35
5.1.6 Media Storage 36
5.1.7 Waste Disposal 36
5.1.8 Off-Site Back-Up 36
5.2 PROCEDURAL CONTROLS 37
5.2.1 Trusted Roles 37
5.2.2 Number of Persons Required per Task 38
5.2.3 Identification and Authentication for Each Role 38
5.2.4 Roles Requiring Separation of Duties 39
5.3 PERSONNEL CONTROLS 39
5.3.1 Qualification, Experience and Clearance Requirements 39
5.3.2 Background Check Procedures 39
5.3.3 Training Requirements 39
5.3.4 Retraining Frequency and Requirements 39
5.3.5 Job Rotation Frequency and Sequence 40
5.3.6 Sanctions for Unauthorised Actions 40
5.3.7 Independent Contractor Requirements 40
5.3.8 Documentation Supplied to Personnel 40
5.4 AUDIT LOGGING PROCEDURES 40
5.4.1 Types of Events Recorded 40
5.4.2 Frequency of Processing Log 41
5.4.3 Retention Period for Audit Log 42
5.4.4 Protection of Audit Log 42
5.4.5 Audit Log Back-Up Procedures 43
5.4.6 Audit Collection System (Internal or External) 43
5.4.7 Notification to Event-Causing Subject 43
5.4.8 Vulnerability Assessments 44
5.5 RECORDS ARCHIVAL 44
5.5.1 Types of Records Archived 44
5.5.2 Retention Period for Archive 44
5.5.3 Protection of Archive 44

5.5.4 Archive Back-Up Procedures 45
5.5.5 Requirements for Time-Stamping of Records 45
5.5.6 Archive Collection System (Internal or External) 45
5.5.7 Procedures to Obtain and Verify Archive Information 45
5.6 KEY CHANGEOVER 45
5.6.1 Organisation Certificate Key Changeover 45
5.6.2 OCA Key Changeover 46
5.6.3 Subscriber Key Changeover 46
5.7 COMPROMISE AND DISASTER RECOVERY 47
5.7.1 Incident and Compromise Handling Procedures 47
5.7.2 Computing Resources, Software and/or Data are Corrupted 48
5.7.3 Entity Private Key Compromise Procedures 48
5.7.4 Business Continuity Capabilities after a Disaster 48
5.8 CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY TERMINATION 48
6 TECHNICAL SECURITY CONTROLS 49
6.1 KEY PAIR GENERATION AND INSTALLATION 49
6.1.1 Key Pair Generation 49
6.1.2 Private Key Delivery to Subscriber 49
6.1.3 Public Key Delivery to Certificate Issuer 49
6.1.4 OCA Public Key Delivery to Relying Parties 50
6.1.5 Key Sizes 50
6.1.6 Public Key Parameters Generation and Quality Checking 50
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 50
6.1.7 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 51
6.2.1 Cryptographic Module Standards and Controls 51
6.2.2 Private Key (n out of m) Multi-Person Control 52
6.2.3 Private Key Escrow 52
6.2.4 Private Key Back-Up 52
6.2.5 Private Key Archival 53
6.2.6 Private Key Transfer into or from a Cryptographic Module 53
6.2.7 Private Key Storage on Cryptographic Module 53
6.2.8 Method of Activating Private Key 53
6.2.9 Method of Deactivating Private Key 53
6.2.10 Method of Destroying Private Key 54
6.2.11 Cryptographic Module Rating 54
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 54
6.3.1 Public Key Archival 54
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 54
6.4 ACTIVATION DATA 55
6.4.1 Activation Data Generation and Installation 55
6.4.2 Activation Data Protection 55
6.4.3 Other Aspects of Activation Data 55
6.5 COMPUTER SECURITY CONTROLS 55
6.5.1 Specific Computer Security Technical Requirements 55
6.5.2 Computer Security Rating 56
6.6 LIFE-CYCLE TECHNICAL CONTROLS 56
6.6.1 System Development Controls 56
6.6.2 Security Management Controls 57
6.6.3 Life-Cycle Security Controls 57
6.7 NETWORK SECURITY CONTROLS 57
6.7.1 Use of Offline Root OCA 57

6.7.2 Protection Against Attack 57
6.7.3 Separation of Issuing OCA 57
6.7.4 Health Check of OCA Systems 58
6.8 TIME-STAMPING 58
6.8.1 Use of Time-Stamping 58
7 CERTIFICATE, CRL AND OCSP PROFILES 58
7.1 CERTIFICATE PROFILES 58
7.1.1 Version Number(s) 58
7.1.2 Certificate Extensions 58
7.1.3 Algorithm Object Identifiers 58
7.1.4 Name Forms 59
7.1.5 Name Constraints 59
7.1.6 Certificate Policy Object Identifier 59
7.1.7 Usage of Policy Constraints Extension 59
7.1.8 Policy Qualifiers Syntax and Semantics 59
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 59
7.2 CRL PROFILE 59
7.2.1 Version Number(s) 59
7.2.2 CRL and CRL Entry Extensions 59
7.3 OCSP PROFILE 59
7.3.1 Version Number(s) 59
7.3.2 OCSP Extensions 60
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 61
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 61
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 61
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 61
8.4 TOPICS COVERED BY ASSESSMENT 61
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 61
8.6 COMMUNICATION OF RESULTS 61
9 OTHER BUSINESS AND LEGAL MATTERS 62
9.1 FEES 62
9.1.1 Certificate Issuance or Renewal Fees 62
9.1.2 Organisation Certificate Access Fees 62
9.1.3 Revocation or Status Information Access Fees 62
9.1.4 Fees for Other Services 62
9.1.5 Refund Policy 62
9.2 FINANCIAL RESPONSIBILITY 62
9.2.1 Insurance Coverage 62
9.2.2 Other Assets 62
9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects 62
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 63
9.3.1 Scope of Confidential Information 63
9.3.2 Information not within the Scope of Confidential Information 63
9.3.3 Responsibility to Protect Confidential Information 63
9.4 PRIVACY OF PERSONAL INFORMATION 63
9.4.1 Privacy Plan 63
9.4.2 Information Treated as Private 63
9.4.3 Information not Deemed Private 63
9.4.4 Responsibility to Protect Private Information 63
9.4.5 Notice and Consent to Use Private Information 63
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 63
9.4.7 Other Information Disclosure Circumstances 63
9.5 INTELLECTUAL PROPERTY RIGHTS 64

9.6 REPRESENTATIONS AND WARRANTIES 64
9.6.1 Certification Authority Representations and Warranties 64
9.6.2 Registration Authority Representations and Warranties 64
9.6.3 Subscriber Representations and Warranties 64
9.6.4 Relying Party Representations and Warranties 64
9.6.5 Representations and Warranties of Other Participants 64
9.7 DISCLAIMERS OF WARRANTIES 64
9.8 LIMITATIONS OF LIABILITY 64
9.9 INDEMNITIES 64
9.10 TERM AND TERMINATION 64
9.10.1 Term 64
9.10.2 Termination of Organisation Certificate Policy 65
9.10.3 Effect of Termination and Survival 65
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 65
9.11.1 Subscribers 65
9.11.2 Organisation Certification Authority 65
9.11.3 Notification 65
9.12 AMENDMENTS 65
9.12.1 Procedure for Amendment 65
9.12.2 Notification Mechanism and Period 65
9.12.3 Circumstances under which OID Must be Changed 65
9.13 DISPUTE RESOLUTION PROVISIONS 65
9.14 GOVERNING LAW 66
9.15 COMPLIANCE WITH APPLICABLE LAW 66
9.16 MISCELLANEOUS PROVISIONS 66
9.16.1 Entire Agreement 66
9.16.2 Assignment 66
9.16.3 Severability 66
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 66
9.16.5 Force Majeure 66
9.17 OTHER PROVISIONS 66
9.17.1 Organisation Certificate Policy Content 66
9.17.2 Third Party Rights 66
Annex A: Definitions and Interpretation 67
Annex B: OCA CERTIFICATE AND ORGANISATION CERTIFICATE PROFILES 73

1 INTRODUCTION

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

- shall be known as the "**Organisation 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) Organisation Certificates; and

(ii) OCA 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

(D) 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. 8641679.1.2.1.1.

1.3 SMKI PARTICIPANTS

1.3.1 The Organisation Certification Authority

(A) The definition of Organisation 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 an Organisation Certificate must be an Organisation and be identified in the `subject` field of the Organisation Certificate Profile in accordance with Annex B.

(B) The Subject of an OCA Certificate must be the entity identified by the

`subject` field of the Root OCA Certificate Profile or Issuing OCA Certificate Profile (as the case may be) in accordance with Annex B.

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

1.3.5 Relying Parties

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

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

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

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

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 ORGANISATION CERTIFICATES AND OCA CERTIFICATES

1.4.1 Appropriate Certificate Uses

(A) The OCA shall ensure that Organisation Certificates are Issued only:

(i) to Eligible Subscribers; and

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

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

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

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

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

1.4.2 Prohibited Certificate Uses

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

1.5 POLICY ADMINISTRATION

1.5.1 Organisation Administering the Document

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

1.5.2 Contact Person

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

1.5.3 Person Determining Organisation CPS Suitability for the Policy

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

1.5.4 Organisation CPS Approval Procedures

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

1.5.5 Registration Authority Policies and Procedures

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

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

(ii) each OCA Certificate;

(iii) each version of the SMKI RAPP;

(iv) each version of the SMKI Recovery Procedure;

(v) the latest version of the Organisation CRL;

(vi) the latest version of the Organisation ARL; and

(vii) 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 OCA 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 OCA shall ensure that:

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

(ii) each OCA Certificate is lodged to the SMKI Repository promptly on

being Issued;

(iii) 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;

(iv) 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;

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

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

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

2.4 ACCESS CONTROLS ON REPOSITORIES

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

(A) Provision is made in the SMKI RAPP to ensure that the name of the entity that is the Subject of each Certificate 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 OCA 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 OCA 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 or an equivalent cryptographic mechanism.

3.2.2 Authentication of Organisation Identity

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

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

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

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

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

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

3.2.3 Authentication of Individual Identity

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

persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to Level 3 (Verified) pursuant to the CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

3.2.4 Non-verified Subscriber Information

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

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

3.2.5 Validation of Authority

See Part 3.2.2 of this Policy.

3.2.6 Criteria for Interoperation

[*Not applicable in this Policy*]

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

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

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

3.3.2 Identification and Authentication for Re-Key after Revocation

[*Not applicable in this Policy*]

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

3.4.1 Authentication for Certificate Revocation Requests

(A) Provision is made in the SMKI RAPP in relation to procedures designed to ensure the Authentication of persons who submit a Certificate Revocation

Request and verify that they are authorised to submit that request.

4 CERTIFICATE 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 an Organisation 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; and

(ii) in respect of an OCA Certificate, the procedure to be followed by an Eligible Subscriber in order to obtain an OCA Certificate.

4.1.2 Enrolment Process and Responsibilities

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

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

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

4.1.3 Enrolment Process for the Registration Authority and its Representatives

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

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

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

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

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

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the SMKI RAPP in relation to the Authentication by the OCA 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, this Policy or any other provision of the Code, the OCA:

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

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

(B) Where any Certificate Signing Request satisfies the requirements set out in the SMKI RAPP, this Policy or any other provision of the Code, the OCA 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 OCA is made in Section L8 of the Code (SMKI Performance Standards and Demand Management).

4.3 CERTIFICATE ISSUANCE

4.3.1 OCA Actions during Certificate Issuance

(A) The OCA may Issue a Certificate only:

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

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

(B) The OCA shall ensure that:

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

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

(C) An OCA Certificate may only be:

(i) Issued by the OCA; and

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

(D) An Organisation Certificate may only be:

(i) Issued by the OCA; and

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

(E) The OCA shall not Issue:

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

(ii) an Organisation Certificate using an Issuing OCA Private Key after the expiry of the Validity Period of an Issuing OCA Certificate containing

the Public Key associated with that Private Key; or

(iii) any 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 (except that the OCA may Issue an OCA Root Certificate containing the same Public Key in so far as it contains a different, or differently encrypted, Contingency Public Key).

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

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

(i) specify a means by which an Eligible Subscriber may clearly indicate to the OCA its rejection of a Certificate which has been Issued to it; 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.

(B) A Certificate which has been Issued by the OCA 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 OCA shall maintain a record of all Certificates which have been Issued by it and are treated as accepted by a Subscriber.

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

4.4.2 Publication of Certificates by the OCA

(A) Provision in relation to the publication of Certificates is made in Part 2 of this Policy (Publication and Repository Responsibilities) and Section L5 of the Code (The SMKI Repository Service).

4.4.3 Notification of Certificate Issuance by the OCA to Other Entities

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

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

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

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

(ii) this Policy.

4.5.2 Relying Party Public Key and Certificate Usage

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

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances of Certificate Renewal

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

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

4.6.2 Circumstances of Certificate Replacement

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

(i) immediately notify the SMKI PMA;

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

(iii) where the Compromise or suspected Compromise relates to an OCA Private Key (but subject to the provisions of the SMKI Recovery Procedure):

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

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

(c) promptly both notify the SMKI PMA and, subject to the provisions of the SMKI Recovery Procedure, verifiably destroy the OCA Private Key Material.

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

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

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

(C) A Subscriber for an Organisation Certificate may request a replacement for that Certificate at any time by applying for the Issue of a new Organisation 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 OCA

See Part 4.4.2 of this Policy.

4.6.8 Notification of Certificate Issuance by the OCA 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 OCA shall not provide a Certificate Re-Key service.

(C) Where a new Key Pair has been generated for use by the Subject of an Organisation Certificate, the Subscriber for a Certificate which is associated with the previous Key Pair 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 OCA

[*Not applicable in this Policy*]

4.7.7 Notification of Certificate Issuance by the OCA 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 (except to the extent to which it permits the OCA to Issue an OCA Root Certificate containing the same Public Key as a Certificate previously Issued by it, where the Certificates contain different, or differently encrypted, Contingency Public Keys).

(B) Subject to paragraph (A), neither the OCA 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 OCA

[*Not applicable in this Policy*]

4.8.7 Notification of Certificate Issuance by the OCA to Other Entities

[*Not applicable in this Policy*]

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

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

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

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

(B) The OCA must revoke a Certificate upon:

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

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

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

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

(ii) where it has determined that the Subscriber for that Certificate does not

continue to satisfy the criteria set out in this Policy and the SMKI RAPP for being an Authorised Subscriber;

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

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

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

4.9.2 Who can Request Revocation

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

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

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

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

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

4.9.3 Procedure for Revocation Request

(A) Provision is made in the SMKI RAPP in relation to the procedure for submitting and processing a Certificate Revocation Request.

(B) On receiving a Certificate Revocation Request, the OCA shall take

reasonable steps to:

(i) Authenticate the Subscriber making that request;

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

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

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

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

4.9.4 Revocation Request Grace Period

[*Not applicable in this Policy*]

4.9.5 Time within which OCA must process the Revocation Request

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

4.9.6 Revocation Checking Requirements for Relying Parties

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

4.9.7 CRL Issuance Frequency (if applicable)

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

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

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

(B) Each version of the Organisation ARL shall be valid until the date which is up to 13 months after the date on which that version of the Organisation ARL is lodged in the SMKI Repository.

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

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

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

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

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

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

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

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

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

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

(I) The OCA shall retain a copy of the information contained in all versions of the Organisation CRL and Organisation ARL, together with the dates and

times between which each such version was valid. This information shall be made available as soon as is reasonably practicable, on receipt of a request, to the Panel, the SMKI PMA, any Subscriber or any Relying Party.

4.9.8 Maximum Latency for CRLs (if applicable)

See Part 4.9.7 of this Policy.

4.9.9 On-line Revocation/Status Checking Availability

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

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

4.9.10 On-line Revocation Checking Requirements

[*Not applicable in this Policy*]

4.9.11 Other Forms of Revocation Advertisements Available

[*Not applicable in this Policy*]

4.9.12 Special Requirements in the Event of Key Compromise

See Part 4.6.2 of this Policy.

4.9.13 Circumstances for Suspension

[*Not applicable in this Policy*]

4.9.14 Who can Request Suspension

[*Not applicable in this Policy*]

4.9.15 Procedure for Suspension Request

[*Not applicable in this Policy*]

4.9.16 Limits on Suspension Period

[*Not applicable in this Policy*]

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

[*Not applicable in this Policy*]

4.10.2 Service Availability

(A) In circumstances in which:

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

(ii) the SMKI Repository Service is unavailable,

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

(B) In circumstances in which:

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

(ii) the SMKI Repository Service is unavailable,

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

4.10.3 Optional Features

[*Not applicable in this Policy*]

4.11 END OF SUBSCRIPTION

[*Not applicable in this Policy*]

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policies and Practices

(A) This Policy does not support Key Escrow.

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

(B) The OCA shall ensure that:

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

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

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

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

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

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

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

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

containers accessible only to appropriately authorised individuals.

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

5.1.2 Physical Access

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

5.1.4 Water Exposure

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

(A) The OCA shall ensure that the Organisation 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 OCA.

5.1.7 Waste Disposal

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

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

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

5.1.8 Off-Site Back-Up

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

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

(C) The OCA 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 Organisation CPS, including when being transmitted for the purposes of Back-Up; and

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

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

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

(iii) no individual member of OCA Personnel is capable, by acting alone,

of engaging in any action by means of which the OCA Systems may be Compromised to a material extent; and

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

5.2.2 Number of Persons Required per Task

(A) The OCA shall ensure that the Organisation CPS incorporates provisions designed to establish:

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

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

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

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

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

(i) OCA Systems administration;

(ii) OCA Systems operations;

(iii) OCA Systems security; and

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

(B) The OCA shall ensure that all OCA 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 OCA shall ensure that the Organisation CPS incorporates appropriate

provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of OCA Personnel.

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorised Actions

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

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

(A) The OCA shall ensure that all OCA 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 Organisation CPS; and

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

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

(A) The OCA shall ensure that:

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

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

(a) the activities of OCA Personnel;

(b) the use of OCA equipment;

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

(d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the OCA 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 OCA shall ensure that:

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

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

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

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

(iii) it monitors the OCA Systems in compliance with:

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

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

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

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

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

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

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

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

5.4.3 Retention Period for Audit Log

(A) The OCA 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 OCA shall ensure that:

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

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

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

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

5.4.5 Audit Log Back-Up Procedures

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

(B) The OCA 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 Organisation 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 OCA shall ensure that the Organisation 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 OCA shall ensure that the Organisation 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 OCA Systems.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

(A) The OCA 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 OCA 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 OCA 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 OCA shall ensure that the Organisation 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 OCA shall ensure that the Organisation 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 OCA 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 OCA's operations.

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

5.6 KEY CHANGEOVER

5.6.1 Organisation Certificate Key Changeover

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

5.6.2 OCA Key Changeover

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

(i) either:

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

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

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

(iii) generate a new Key Pair;

(iv) ensure that any relevant Certificate subsequently Issued by it is Issued using the OCA 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 OCA:

(a) Issue a new relevant OCA Certificate; and

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

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

5.6.3 Subscriber Key Changeover

(A) Where:

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

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

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

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

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

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

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

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

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

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

(C) The OCA shall ensure that the Organisation 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 OCA Private Key or any part of the OCA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The OCA 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 OCA 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 OCA shall ensure that the Organisation 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 OCA, the Issuing OCA and the Registration Authority.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(A) The OCA 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 such Key Pair; 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 OCA shall not generate any Private Key or Public Key other than an OCA Key.

6.1.2 Private Key Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate Issuer

(A) The OCA shall ensure that the Organisation 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 OCA and Issuing OCA; and

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

6.1.4 OCA Public Key Delivery to Relying Parties

(A) The OCA shall ensure that the Organisation CPS incorporates provisions:

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

(ii) designed to ensure that the OCA 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 OCA 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 OCA 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 OCA shall ensure that each Certificate that is Issued by it has a `keyUsage` field in accordance with RFC5759 and RFC5280.

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

(i) `digitalSignature`; or

(ii) `keyAgreement`.

(C) The OCA shall ensure that each OCA Certificate that is Issued by it has a `keyUsage` of either:

(i) `keyCertSign`; or

(ii) `CRLSign`.

(D) The OCA shall ensure that no `keyUsage` values may be set in an Organisation Certificate or OCA 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 OCA shall ensure that all OCA 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 OCA shall ensure that all OCA 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 OCA shall ensure that no OCA 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 OCA 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 Organisation CPS; and

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

6.2.4 Private Key Back-Up

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

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

6.2.10 Method of Destroying Private Key

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

(B) The OCA shall ensure that no OCA 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 OCA 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 OCA shall ensure that it archives OCA 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 OCA shall ensure that the Validity Period of each Certificate Issued by it shall be as follows:

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

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

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

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

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

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

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

(B) The OCA 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 OCA Keys; and

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

6.4.2 Activation Data Protection

(A) The OCA shall ensure that the Organisation 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 OCA shall ensure that the Organisation 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 OCA;

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

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

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

(v) the audit of security related events; and

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

6.5.2 Computer Security Rating

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

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

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

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

6.7.2 Protection Against Attack

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

(A) The DCC shall ensure that, where its functions as the Issuing OCA are carried out on a part of the OCA Systems that is connected to an external network,

they are carried out on a System that is Separated from all other OCA Systems.

6.7.4 Health Check of OCA Systems

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

6.8 TIME-STAMPING

6.8.1 Use of Time-Stamping

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

(B) The OCA shall ensure that the Organisation 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 OCA.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILES

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

7.1.1 Version Number(s)

[*Not applicable in this Policy*]

7.1.2 Certificate Extensions

[*Not applicable in this Policy*]

7.1.3 Algorithm Object Identifiers

[*Not applicable in this Policy*]

7.1.4 Name Forms

[*Not applicable in this Policy*]

7.1.5 Name Constraints

[*Not applicable in this Policy*]

7.1.6 Certificate Policy Object Identifier

[*Not applicable in this Policy*]

7.1.7 Usage of Policy Constraints Extension

[*Not applicable in this Policy*]

7.1.8 Policy Qualifiers Syntax and Semantics

[*Not applicable in this Policy*]

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

[*Not applicable in this Policy*]

7.2 CRL PROFILE

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

(A) The OCA shall notify Parties of the profile of the Organisation CRL and of any Organisation CRL extensions.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

[*Not applicable in this Policy*]

7.3.2 OCSP Extensions

[*Not applicable in this Policy*]

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

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

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

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

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4 TOPICS COVERED BY ASSESSMENT

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

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

8.6 COMMUNICATION OF RESULTS

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

9 OTHER BUSINESS AND LEGAL MATTERS

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

9.1 FEES

See the statement at the beginning of this Part.

9.1.1 Certificate Issuance or Renewal Fees

See the statement at the beginning of this Part.

9.1.2 Organisation Certificate Access Fees

See the statement at the beginning of this Part.

9.1.3 Revocation or Status Information Access Fees

See the statement at the beginning of this Part.

9.1.4 Fees for Other Services

See the statement at the beginning of this Part.

9.1.5 Refund Policy

See the statement at the beginning of this Part.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

See the statement at the beginning of this Part.

9.2.2 Other Assets

See the statement at the beginning of this Part.

9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

See the statement at the beginning of this Part.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.2 Information not within the Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.3 Responsibility to Protect Confidential Information

See the statement at the beginning of this Part.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

See the statement at the beginning of this Part.

9.4.2 Information Treated as Private

See the statement at the beginning of this Part.

9.4.3 Information not Deemed Private

See the statement at the beginning of this Part.

9.4.4 Responsibility to Protect Private Information

See the statement at the beginning of this Part.

9.4.5 Notice and Consent to Use Private Information

See the statement at the beginning of this Part.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

See the statement at the beginning of this Part.

9.4.7 Other Information Disclosure Circumstances

See the statement at the beginning of this Part.

9.5 INTELLECTUAL PROPERTY RIGHTS

See the statement at the beginning of this Part.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 Certification Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.2 Registration Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.3 Subscriber Representations and Warranties

See the statement at the beginning of this Part.

9.6.4 Relying Party Representations and Warranties

See the statement at the beginning of this Part.

9.6.5 Representations and Warranties of Other Participants

See the statement at the beginning of this Part.

9.7 DISCLAIMERS OF WARRANTIES

See the statement at the beginning of this Part.

9.8 LIMITATIONS OF LIABILITY

See the statement at the beginning of this Part.

9.9 INDEMNITIES

See the statement at the beginning of this Part.

9.10 TERM AND TERMINATION

9.10.1 Term

See the statement at the beginning of this Part.

9.10.2 Termination of Organisation Certificate Policy

See the statement at the beginning of this Part.

9.10.3 Effect of Termination and Survival

See the statement at the beginning of this Part.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 Subscribers

See the statement at the beginning of this Part.

9.11.2 Organisation Certification Authority

See the statement at the beginning of this Part.

9.11.3 Notification

See the statement at the beginning of this Part.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

See the statement at the beginning of this Part.

9.12.2 Notification Mechanism and Period

See the statement at the beginning of this Part.

9.12.3 Circumstances under which OID Must be Changed

See the statement at the beginning of this Part.

9.13 DISPUTE RESOLUTION PROVISIONS

See the statement at the beginning of this Part.

9.14 GOVERNING LAW

See the statement at the beginning of this Part.

9.15 COMPLIANCE WITH APPLICABLE LAW

See the statement at the beginning of this Part.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

See the statement at the beginning of this Part.

9.16.2 Assignment

See the statement at the beginning of this Part.

9.16.3 Severability

See the statement at the beginning of this Part.

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

See the statement at the beginning of this Part.

9.16.5 Force Majeure

See the statement at the beginning of this Part.

9.17 OTHER PROVISIONS

9.17.1 Organisation Certificate Policy Content

See the statement at the beginning of this Part.

9.17.2 Third Party Rights

See the statement at the beginning of this Part.

Annex A: Definitions and Interpretation

In this Policy, except where the context otherwise requires -

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

Certificate	means either an Organisation Certificate or an OCA Certificate.
Certificate Profile	means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.
Certificate Re-Key	means a change to the Public Key contained within a Certificate bearing a particular serial number.
Certificate Revocation Request	means a request for the revocation of a Certificate by the OCA, submitted by the Subscriber for that Certificate to the OCA in accordance with the SMKI RAPP and this Policy.
Certificate Signing Request	means a request for a Certificate submitted by an Eligible Subscriber in accordance with the SMKI RAPP.
DCA	has the meaning given to that expression in Appendix A of the Code (Device Certificate Policy).
DCA Systems	has the meaning given to that expression in Appendix A of the Code (Device Certificate Policy).
Eligible Subscriber	means: (a) in relation to an Organisation Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.18 of the Code (Organisation Certificates); and (b) in relation to an OCA Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.19 of the Code (OCA Certificates).
Entity Identifier	means a User ID, RDP ID or a DCC ID as required by the context.

Issue	means the act of the OCA, in its capacity as the Root OCA or Issuing OCA, 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 Organisation Certification Authority (or **Issuing OCA**)	means the DCC exercising the function of Issuing Organisation Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function.
Issuing OCA Certificate	means a certificate in the form set out in the Issuing OCA Certificate Profile in accordance with Annex B, and Issued by the Root OCA to the Issuing OCA in accordance with this Policy.
Issuing OCA Private Key	means a Private Key which is stored and managed by the OCA acting in its capacity as the Issuing OCA.
Issuing OCA Public Key	means the Public Key which is part of a Key Pair with an Issuing OCA 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 Certificate	means either a Root OCA Certificate or an Issuing OCA Certificate.
OCA Key	means any Private Key or a Public Key generated by the OCA for the purposes of complying with its obligations under the Code.

OCA Private Key	means either a Root OCA Private Key or an Issuing OCA Private Key.
OCA Systems	means the Systems used by the OCA in relation to the SMKI Services.
Organisation Authority Revocation List (or **ARL**)	means a list, produced by the OCA, of all OCA Certificates that have been revoked in accordance with this Policy.
Organisation Certificate	means a certificate in the form set out in the Organisation Certificate Profile in accordance with Annex B, and Issued by the Issuing OCA in accordance with this Policy.
Organisation Certificate Revocation List (or **CRL**)	means a list, produced by the OCA, of all Organisation Certificates that have been revoked in accordance with this Policy.
Organisation Certification Authority (or **OCA**)	means the DCC, acting in the capacity and exercising the functions of one or more of: (a) the Root OCA; (b) the Issuing OCA; and (c) the Registration Authority.
Private Key Material	in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.
Registration Authority	means the DCC exercising the function of receiving and processing Certificate Signing Requests made in accordance with the SMKI RAPP.
Registration Authority Manager	means either a director of the DCC or any other person who may be identified as such in accordance with the SMKI RAPP.

Registration Authority Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the Registration Authority.
Relying Party	means a person who, pursuant to the Code, receives and relies upon a Certificate.
Root Organisation Certification Authority (or **Root OCA**)	means the DCC exercising the function of Issuing OCA Certificates to the Issuing OCA and storing and managing Private Keys associated with that function.
Root OCA Certificate	means a certificate in the form set out in the Root OCA Certificate Profile in accordance with Annex B and self-signed by the Root OCA in accordance with this Policy.
Root OCA Private Key	means a Private Key which is stored and managed by the OCA acting in its capacity as the Root OCA.
Security Related Functionality	means the functionality of the OCA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of that System.
Subject	means: (a) in relation to an Organisation Certificate, the Organisation identified by the `subject` field of the Organisation Certificate Profile in Annex B; and (b) in relation to an OCA Certificate, the globally unique name of the Root OCA or Issuing OCA 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 OCA that: (a) where required, provides an appropriately precise time-stamp in the format required by this Policy; and (b) relies on a time source that is: (i) accurate; (ii) determined in a manner that is independent of any other part of the OCA 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: OCA Certificate and Organisation Certificate Profiles

End Entity Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which OCA Certificates and Organisation 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 and IETF RFC5280.

Common requirements applicable to OCA Certificates and Organisation Certificates

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

- shall be compliant with IETF RFC 5759 and so with IETF RFC5280.
- for clarity and in adherence with the requirements of IETF RFC5759, all OCA Certificates and Organisation Certificates shall:
    - contain the `authorityKeyIdentifier` extension, except where the Certificate is the Root OCA 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;
- shall, in relation to communications with devices, contain a non-empty subject field which contains an `X520OrganizationalUnitName` whose value is to be expressed as the human-readable two octet hexadecimal representation of the integer Remote Party Role that the Certificate allows the Subject of the Certificate to perform;
- 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 RFC5480;
- 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 Parties and 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 OCA Certificate. Note this exception only applies where Remote Party Role as specified in the `X520OrganizationalUnitName` part of the `subject` field = root;
- 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 expiration date as per IETF RFC 5280 Section 4.1.2.5.

Requirements applicable to Organisation Certificates only

All Organisation Certificates that are issued by the OCA shall:

- within the `subject` field, in addition to other attributes, contain an `AttributeTypeAndValue` structure whose type shall be `id-at-uniqueIdentifier {joint-iso-itu-t(2) ds(5) attributeType(4) uniqueIdentifier(45)}` and whose value shall be the 8 octet Entity Identifier of the subject of the Certificate;
- 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 of this Policy under which the Certificate is issued.

Requirements applicable to the Root OCA and Issuing OCA

All OCA Certificates issued by the OCA shall:

- have globally unique `subject` field contents;
- contain a single public key except for the Root-CA where there shall be two public keys. The second public key shall be referred to as the Contingency Key and shall be present in the `WrappedApexContingencyKey` extension with the meaning of IETF RFC5934. The Contingency Key shall be encrypted as per the requirements of the GBCS;
- contain a `keyUsage` extension marked as critical and defined as:
  - `keyCertSign`; and
  - `cRLSign`;
- for Issuing OCA Certificates, contain at least one `CertPolicyID` in the `certificatePolicies` extension that refers to the OID of this Policy under which the Certificate is issued;
- for the Root OCA Certificate, contain a single `CertPolicyID` in the `certificatePolicies` extension that refers to the OID for `anyPolicy`;
- for Issuing OCA Certificates, contain the `basicConstraints` extension, with values `cA=True`, and `pathLen=0`. This extension shall be marked as critical;
- for the Root OCA Certificate, contain the basicConstraints extension, with the value `cA=True` and `pathLen absent` (unlimited). This extension shall be marked as critical.

Organisation 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 OCA of up to 4 Octets (as defined in the Issuing OCA Certificate Profile)	
keyIdentifier in Authoritykeyidentifier (the "Subject 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 Organisation Certificate	
notAfter	Time	Expiry time of the Certificate	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Name of the Subject of up to 16 Octets	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-organizationalUnitName (the "Subject X520 Organizational Unit Name")	UTF8String	Remote Party Role of the subject of the Certificate	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-uniqueIdentifier	UniqueIdentifier	The 64 bit Entity Identifier of the subject of the Certificate	

(the "Subject Unique Identifier")			
`subjectPublicKeyInfo`	`SubjectPublicKeyInfo`	The subject's Public Key	
`extensions`	`Extensions`	Critical and non-critical extensions	
`signatureAlgorithm`	`AlgorithmIdentifier`	SHA256 with ECDSA	
`signatureValue`	`BIT STRING`	Subject Organisation Certificate signature	

Interpretation

`version`

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

`serialNumber`

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

`signature`

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

Issuer X520 Common Name

The name of the signer of the Organisation Certificate. This will be the gloablly unique name of the Issuing OCA of up to 4 Octets (as defined in the Issuing OCA 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 Organisation Certificates.

Subject Key Identifier

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

`validity`

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

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

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

`notBefore`

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

`notAfter`

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

Subject X520 Common Name

This field shall contain a unique X.500 Distinguished Name (DN). This should be the unique trading name of the Organisation of up to 16 Octets.

Subject X520 Organizational Unit Name

The Subject X520 Organizational Unit Name attribute of `subject` shall be populated with the Remote Party Role Code that the Certificate allows the subject of the Certificate to perform.

Subject Unique Identifier

This shall be populated with the 64 bit Entity Identifier of the subject of the Certificate

`subjectPublicKeyInfo`

The Organisation 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` Organisation 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 Organisation 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 OCA signature algorithm used to sign this Organisation Certificate is as defined under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Issuing OCA's signature of the Organisation Certificate shall be computed using the Issuing OCA'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`

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

- `certificatePolicy`

- 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 and 6318. 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 OCA 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 Root OCA of up to 4 Octets	
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	
notBefore	Time	Creation time of the Certificate	
notAfter	Time	Expiry time of the Certificate	
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 OCA of up to 4 Octets (same as Issuer name)	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-	UTF8String	Remote Party Role of the subject of the Certificate	

organizationalUnitName (the "Subject X520 Organizational Unit Name")			
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
The extnValue in the extension whose extnID is id-pe-WrappedApexContingencyKey	ApexContingencyKey	The Subject's protected (encrypted) Public Key used for recovery purposes	
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 Organisations 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 OCA that signs the Certificate (self-signed by Root OCA). The serialNumber shall be unique in the scope of Certificates signed by the OCA.

`signature`

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Root OCA 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 OCA of up to 4 Octets. This will be the same as the `subject` as it is self-signed by the Root OCA.

Subject Key Identifier

The `SubjectKeyIdentifier` extension shall 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.

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

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

`notBefore`

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

`notAfter`

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

Subject X520 Common Name

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

Subject X520 Organizational Unit Name

The Subject X520 `OrganizationalUnitName` attribute of `subject` shall be populated with the Remote Party Role Code that the Certificate allows the subject of the Certificate to perform.

`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 `KeyUsage` 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:

o `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 fo the curve choice to be used in OCA 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 OCA signature algorithm used to sign this Certificate as defined in section under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Root OCA's signature of the Certificate shall be computed using the Root OCA'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 shall contain the `extensions` described below. They SHOULD NOT contain any additional `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 and 6318. 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 OCA 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 `AttributeTypeAnd`	`UTF8String`	Globally unique name of Root OCA of up to 4	

`Value` structure within the `subject` field whose `type` is `id-at-commonName` (the "Issuer X520 Common Name")		Octets (as defined in the Root OCA 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`	Expiry time of the Certificate	
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 OCA of up to 4 Octets	

The `value` field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-organizationalUnitName` (the "Subject X520 Organizational Unit Name")	`UTF8String`	Remote Party Role of the Subject of the Certificate	
`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 Root OCA that signs the Certificate. The serialNumber shall be unique in the scope of Certificates signed by the Root OCA.

signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing OCA 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 OCA of up to 4 Octets (as defined in the Root OCA Certificate Profile).

Subject Key Identifier

The SubjectKeyIdentifier extension shall 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 Organisation 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.

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

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

notBefore

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

notAfter

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

Subject X520 Common Name

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

Subject X520 Organizational Unit Name

The Subject X520 Organizational Unit Name attribute of subject shall be populated with the Remote Party Role Code that the Certificate allows the subject of the Certificate to perform.

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 KeyUsage 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 fo 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 OCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Root OCA's signature of the Certificate shall be computed using the Root OCA'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`

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 and 6318. 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.