Aviareto Certificate Policy

Version 1.0 March 2022

CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

A Certificate Policy (CP) is a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements. A Certificate Policy is supported by a Certification Practice Statement ("CPS"). The responsibility for this Certificate Policy lies with a body known as the Policy Authority and any queries regarding the content of this Certificate Policy should be directed to the Policy Authority.

The capitalised and abbreviated terms used throughout this document are explained in the Glossary of Terms at http://certpolicy.aviareto.aero/policy and in Appendix 1 to this Certificate Policy.

This Certificate Policy is structured according to the guidelines provided by IETF RFC 3647 with extensions and modifications defined where appropriate.

The Issuing Authority that Issues Certificates in accordance with this Certificate Policy has made its own stipulations regarding Participants, further restrictions on usage of Certificates, additional liability provisions, etc. These stipulations are published by the Issuing Authority in this Certificate Policy and in a document termed a PKI Disclosure Statement (PDS), which serves as the highest-level vehicle by which provisions affecting Subscribers and Relying Parties are defined. Any PKI Disclosure Statement supporting this Certificate Policy incorporates this Certificate Policy by reference. All Certificates Issued under this Certificate Policy shall contain a reference to where the relevant PKI Disclosure Statement published by the Issuing Authority and associated with this Certificate Policy may be found.

This Certificate Policy defines a Public Key Infrastructure and in conjunction with the relevant PKI Disclosure Statement, specifies:

- Who can participate in the Public Key Infrastructure defined by this Certificate Policy
- The primary rights, obligations and liabilities of the parties governed by this Certificate Policy
- The purposes for which Certificates Issued under this Certificate Policy may be used
- Minimum requirements to be observed in the issuance, management, usage and reliance upon Certificates

1.2 DOCUMENT NAME AND IDENTIFICATION

The certificate policy document on which this Certificate Policy is based is and remains the property of Aviareto Limited at all times and made available through Entrust (Europe) Limited. Entrust (Europe) Limited is registered with the Internet Address Naming Authority (IANA) and has been assigned an Object Identifier ("OID") of 1.3.6.1.4.1.5237. Aviareto's OID is 1.2.826.0.1.3403634.106.1.1

This Certificate Policy has also been assigned an OID as identified in Section 12 of the PKI Disclosure Statements under this Certificate Policy.

1.3 PKI PARTICIPANTS

An Issuing Authority has an obligation to operate a PKI in accordance with the Certificate Policy it defines and publishes. The Issuing Authority does not, however, have to conduct all aspects of PKI operations itself. There are sets of functions that can be logically and conveniently grouped and delegated. This allows PKI services to align with business models, including the outsourcing of some or all of the PKI services to Participants.

There is not necessarily a one-to-one correlation between roles and Participants. Any Participant may perform one or more roles in any particular PKI. Each Participant operates to fulfil clearly defined roles. Typically, these roles are:

- Policy Authority
- Trust Service Providers
    - Issuing Authority
    - Certificate Manufacturer
    - Registration Authority (or Registrar)
    - Repository
- End-Entities
    - Subscriber
    - Subject
    - Relying Party

Under this scheme, End-Entities only have a business relationship with the Issuing Authority. These relationships are defined by the Subscriber Agreements and Relying Party Agreements between the End-Entities and the Issuing Authority. In all matters, under this PKI, the End-Entity relationship is with the Issuing Authority.

Subjects may hold Certificates on behalf of Subscribers. In all cases however, the business relationship with the Issuing Authority is held by the Subscriber.

The requirements placed upon Participants providing Trust Services which support the Issuing Authority are controlled by the provisions of this Certificate Policy and any contractual arrangements between them and the Issuing Authority.

In any case of non-compliance with this Certificate Policy, the Issuing Authority will determine the steps to be taken. It may refer matters to the Policy Authority which has overall and final control over the content of the Certificate Policy and related documentation.

These roles, that collectively comprise the PKI community governed by this Certificate Policy, are described in the remainder of this Section. The descriptions in this Section are illustrative. The specific roles and obligations for Participants are defined elsewhere in this Certificate Policy.

1.3.1 CERTIFICATION AUTHORITIES

Certification Authorities are the entities that Issue Certificates i.e. trust service providers. Within the scope of the model outlined, Certification Authority is the same entity as the Issuing Authority described in Section 1.3.1.1.

1.3.1.1 ISSUING AUTHORITY

By definition, an Issuing Authority is the entity listed in the Issuer field of a Certificate.

The Issuing Authority has the ultimate responsibility for deciding who may be issued with a Certificate carrying its name as the issuer and is the only entity with which End-Entities have any form of direct or indirect contractual relationship. Whether PKI services are provided by internal resources or are contracted out to external Participants, the provisions of this Certificate Policy apply. The Certificate Policy may be complemented by a contract between the Issuing Authority and Participants providing services.

For the benefit of Subscribers and Relying Parties, the Issuing Authority publishes a summary of important provisions that form a part of this Certificate Policy, together with any further provisions affecting Subscribers and Relying Parties, in documents known as PKI Disclosure Statements.

Issuing Authorities ensure that all Certificates Issued by it under this Certificate Policy shall contain a reference to where the relevant PKI Disclosure Statement and this Certificate Policy are published.

1.3.1.2 CERTIFICATE MANUFACTURER

The Certificate Manufacturer provides operational Certificate management services for the Issuing Authority.

The Certificate Manufacturer is approved by the Issuing Authority to manage Certificates on behalf of the Issuing Authority or other Participants in the PKI governed by this Certificate Policy. It has no authority to make decisions on the Issuance of Certificates, or other aspects of certificate management; it operates under the direct control of the Issuing Authority.

The Certificate Manufacturer must demonstrate compliance with this Certificate Policy. Compliance is documented and controlled via a Certification Practice Statement. Where this is complemented by additional supporting documentation it is referred to generically in the Certificate Policy with the term Certificate Manufacturer Procedures.

1.3.2 REGISTRATION AUTHORITIES

The Registration Authority is responsible for ensuring the eligibility of applicants to be Issued with Certificates together with the accuracy and integrity of required information presented by applicants. The Registration Authority is a delegated function of the Issuing Authority, whose role is to process and approve requests from applicants for the Issue of Certificates or for their Revocation, Suspension, Renewal or Re-Key as detailed elsewhere in this Certificate Policy.

A PKI may operate with a single or multiple Registration Authorities. Each must demonstrate compliance with this Certificate Policy. Compliance is documented and controlled via a Certification Practice Statement. Where this is complemented by additional supporting documentation it is referred to generically in the Certificate Policy with the term "Registration Authority Procedures". Such procedures may vary between Registration Authorities. However, in each case they must support the Certification Practice Statement and fully comply with this Certificate Policy.

The Issuing Authority has approved the Registration Authorities listed in Section 13 of the relevant PKI Disclosure Statement with respect to Certificates governed by this Certificate Policy.

1.3.3 SUBSCRIBERS

A Subscriber is an End-Entity (such as a person or organisation) that has applied for and received a Certificate. It is the Subscriber that contracts with an Issuing Authority for the Issuance of Certificates. The Subscriber bears responsibility for the use of the Private Key associated with the Certificate. The Subscriber may be a Subject acting on its own behalf.

Certificate applicants eligible to be authorised by the approved Registration Authorities as Subscribers for the purposes of this Certificate Policy are identified in Section 15 of the relevant PKI Disclosure Statement.

1.3.4 SUBJECTS

Where a Certificate is Issued for a device or Certificate holder that does not directly contract with the Issuing Authority, the Subscriber or an authorised representative acting on behalf of the Subscriber will accept the terms and conditions , as noted in the relevant PKI Disclosure Statement, on behalf of the Subject that is identified in the Certificate. The Subject must be under the jurisdiction and control of the Subscriber and comply with all relevant aspects of this Certificate Policy and other agreements and obligations undertaken by the Subscriber. In all cases the Subscriber is responsible for compliance with the Certificate Policy and all other obligations applicable to it and the Subject (including without limitation under the Subscriber Agreement).

1.3.5 RELYING PARTIES

A Relying Party is an End-Entity that does not necessarily hold a Certificate but even so, may rely on a Certificate and/or Digital Signatures created using that Certificate.

Eligible RelyingParties for Certificates Issued under this Certificate Policy are specified in Section 16 of the relevant PKI Disclosure Statement.

1.3.6 OTHER PARTICIPANTS

1.3.6.1 POLICY AUTHORITY

The Policy Authority has ultimate responsibility for governance and control over the Issuance, management and usage of Certificates Issued under this Certificate Policy. The Policy Authority is the entity that sets the rules under which the PKI is to be operated.

The Policy Authority can be either a governing body or a designee thereof that is tasked with defining the Certificate Policy in a manner that supports and reflects the needs of the underlying relationships and transactions to be supported by a PKI.

The Policy Authority for the purposes of this Certificate Policy is Aviareto Limited through the Aviareto PKI Policy Authority (APPA) as identified in Section 1 of the PKI Disclosure Statements under this Certificate Policy.

1.3.6.2 REPOSITORY

A Repository is a Participant organisation that holds data in support of PKI operations. This includes policy and related documentation, Certificates and Certificate Status Information.

The Repository provides a community wide accessible mechanism where all Participants can access policy and related documentation.

The Repository provides a mechanism by which some Participants can obtain and validate information on Certificates Issued under this Certificate Policy.

The Issuing Authority has approved the Repository identified in Section 14 of the PKI Disclosure Statements under this Certificate Policy, to provide these services.

1.4 CERTIFICATE USAGE

Certificate usage is defined by the Certificate Profile. Certificate Profiles must be approved by the Issuing Authority. Different PKI Disclosure Statements may be issued for different Certificate Profiles as determined by the Issuing Authority.

1.4.1.1 APPROPRIATE CERTIFICATE USES

The categories of transactions, applications, or purposes for which Certificates Issued under this Certificate Policy may be used are defined in Section 2 of the relevant PKI Disclosure Statement.

1.4.1.2 PROHIBITED CERTIFICATE USES

All certificate uses, other than those as set out in 1.4.1.1 above, are expressly prohibited.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANISATION ADMINISTERING THE DOCUMENT

The Policy Authority is responsible for the content of this Certificate Policy and any changes made to it.

Aviareto Limited, as Issuing Authority, shall administer this Certificate Policy. Aviareto Limited may be contacted as follows:

Aviareto Limited	Email: issuingauthority@aviareto.aero
Suite 5, Plaza 255	Web: www.aviareto.aero
Corporate Park 2	
Blanchardstown	Tel: + 353 1 8091470
Dublin 15	

1.5.2 CONTACT PERSON

The Issuing Authority should be contacted regarding the contents of this Certificate Policy.

Contact details are provided in Section 1.5.1 above.

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The Policy Authority determines the suitability of any Certification Practice Statement operating under this Certificate Policy.

In the first instance the Issuing Authority should be contacted regarding the inclusion of additional Certification Authorities to operate within this PKI or interoperation with other PKIs.

Contact details are provided in Section 1.5.1 above.

1.5.4 CPS APPROVAL PROCEDURES

The Policy Authority determines the suitability and approves the use of any Certification Practice Statement which is used to support this Certificate Policy.

1.6 DEFINITIONS AND ACRONYMS

Definitions of the terms used in this Certificate Policy are detailed in the Glossary of Terms contained in Appendix 1.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

An information Repository shall be made available under the terms of this Certificate Policy. The Issuing Authority is the entity with overall responsibility for the operation of a Repository which the Issuing Authority may delegate to Participants providing Trust Services.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The Issuing Authority shall ensure the following items are published for all Participants via the Repository:

- This Certificate Policy with its associated PKI Disclosure Statements.
- Any relevant supporting policy documents and agreements.
- The information that will allow the Authenticity of the Certificate of the Issuing Authority to be verified.
- All CA Certificates issued by the Issuing Authority (including those for sub-ordinate and superior Certificate Authorities, and Cross-certificates for cross-certified PKIs).

The Issuing Authority may make the following available upon request, at its discretion:

- Certificate Status Information for Certificates Issued under this Certificate Policy.

The location of, (or mechanism to obtain access to) this Certificate Policy must be provided in Certificates Issued under this Certificate Policy.

2.3 TIME OR FREQUENCY OF PUBLICATION

Information as listed for publication in Section 2.2 shall be published promptly upon its creation, with the exception that where Certificate Revocation Lists are used to provide Revocation information, they shall be published according to Sections 4.9.7 and 4.9.8 of this Certificate Policy.

2.4 ACCESS CONTROLS ON REPOSITORIES

The Repository must make available the information specified above. However, the Repository may control access to information and grant access only to those Participants with a specific need for the information.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

For Certificates issued to (i) natural persons or (ii) issued to natural persons associated with a legal person, the Issuing Authority X.501 Distinguished Name (DN) in the Issuer field, and the Subject X.501 DN in the Subject field shall comply with IETF PKIX RFC 5280 and ETSI EN 319 412-2, with one exception. The organisational identifier used in the Subject DN, in some instances, contains a unique entity identifier assigned by the Issuing Authority and not in compliance with ETSI EN 319 412-1 clause 5.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The contents of each Certificate Subject name field must have an association with the authenticated name of the Subject. This association may be direct, or where the natural identity of a Subject is required to be hidden, may be recorded elsewhere by the Registration Authority.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The anonymity or pseudonymity of Subscribers is not permitted under this Certificate Policy unless this is explicitly requested by the Issuing Authority responsible for this Certificate Policy. Where permitted, the Registration Authorities operating under this Certificate Policy must record the authenticated real identity of the Subscriber with the anonymised or pseudonymised Subject name.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

For Certificates issued by the Issuing Authority, the following table may be used to interpret the various name forms:

Name of field	[End entity] Signing Identity (Aircraft Protocol)	[End entity] Signing Identity (Trusted Communications Facility)
SubjectName		
CommonName	**<Supplied by IR>** **<Format: AIRU-[IntRegID]-AIRE-[IntRegEntREF]>** **example: AIRU-30-AIRE-86**	**<Supplied by IR>** **<Format: TCFU-[IntRegID]-TCFE-[IntRegEntREF]>** **example: TCFU-30-TCFE-86**
Given name (G)	<Supplied by IR> *example:* Joe	<Supplied by IR> *example:* Joe
Family name (SN)	<Supplied by IR> *example:* Bloggs	<Supplied by IR> *example:* Bloggs
OrganizationIdentifier (2.5.4.97)	<Supplied by IR> *example:* VAT-IE6403536Q *example:* AIRE-nnnnnnnn	<Supplied by IR> *example:* VAT-IE6403536Q *example:* TCFE-nnnnnnnn
SERIALNUMBER	**N/A** *<Omitted 05/07/21 per customer agreement>* *<CN provides per-user uniqueness>*	**N/A** *<Omitted 05/07/21 per customer agreement>* *<CN provides per-user uniqueness>*
OrgUnit	**AIR**	**TCF**
OrgUnit	**Signing Identities**	**Signing Identities**
Org	<Supplied by IR> *example:* Joe Bloggs Corp.	<Supplied by IR> *example:* Joe Bloggs Corp.
Country	<Supplied by IR> *example:* C=GB	<Supplied by IR> *example:* C=GB

3.1.5 UNIQUENESS OF NAMES

Distinguished names must be unique for Certificate Authorities and all Subjects under the jurisdiction of an Issuing Authority. For each Subject any other optional information may be appended to the distinguished name as required for identification or to ensure its uniqueness.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

Neither the Policy Authority nor the Issuing Authority is liable for the inclusion of trademarks, trade names or other information under restricted use. Subscriber Agreements shall require Subscribers to warrant legitimacy of their registration details provided to the Issuing Authority as part of the registration process.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE CONTROL OF PRIVATE KEY

The registration and/or issuance process shall involve a stage in which the natural person applying for the Certificate on behalf of the Subscriber demonstrates sole control of the Private Key. The technical means employed to ensure control of Private Keys will be PKCS#10, other equivalent cryptographic mechanisms, or another process specifically approved by the Policy Authority as specified in the Certification Practice Statement.

3.2.2 AUTHENTICATION OF ORGANISATION IDENTITY

Where an organisation is acting as a Subscriber, or where the organisation is a component of the distinguished name of the Certificate Subject, the identity of the organisation must be established.

Authentication processes must be carried out in accordance with the Certification Practice Statement, including any policies, rules or regulations (or similar) listed in Section 2 of the relevant PKI Disclosure Statement.

Specific requirements for Authentication of organisation identity may be provided in Section 2 of the relevant PKI Disclosure Statement or other community-wide accessible document. The Registration Authority shall define and document the mechanisms used to support the level of Authentication assurance.

The Registration Authority shall verify that each Certificate applicant has a right to obtain that Certificate and, if the Certificate identifies that the Subscriber (or Subject) has particular attributes or privileges, that they are valid.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

The Authentication of Registration Authority Operators must at a minimum satisfy the specific criteria for Authentication specified in the relevant PKI Disclosure Statement. Additionally, the Issuing Authority shall undertake face-to-face Authentication of one or more initial Registration Authority Administrators. An Authenticated and nominated Registration Authority Administrator may undertake face-to-face Authentication of subsequent Registration Authority Administrators.

Authentication processes for the natural person applying for the Certificate on behalf of the Subscriber shall be carried out in accordance with the Certification Practice Statement, including any policies, rules or regulations (or similar) listed in Section 2 of the relevant PKI Disclosure Statement.

The Registration Authority shall verify that each Certificate applicant has a right to obtain that Certificate and, if the Certificate identifies that the Subscriber (or Subject) has particular attributes or privileges, that they are valid.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Use of non-verified information may be included in Certificates governed by this Certificate Policy.

Where non-verified information is incorporated in a Certificate these sources of information must be detailed in the Registration Authority Procedures and approved by the Issuing Authority.

3.2.5 VALIDATION OF AUTHORITY

Validation of authority (i.e. the determination of whether an individual has specific rights, entitlements, or permissions, including the permission to act on behalf of an organisation to obtain a Certificate) must ensure the identity of the individual is Authenticated in accordance with Section 3.2.3 and the authority of the individual is verified in accordance with any policies, rules or regulations (or similar) listed in Section 2 of the relevant PKI Disclosure Statement. Where that authority includes acting on behalf of an organisation, the identity of the organisation must be Authenticated in accordance with Section 3.2.2.

Validation of authority is the responsibility of the Registration Authorities. Validation procedures shall be conducted as described in the Registration Authority Procedures. Details of validation procedures may be published to Participants.

3.2.6 CRITERIA FOR INTEROPERATION

The criteria by which another Certification Authority wishing to operate within, or interoperate with the PKI governed by this Certificate Policy, will be defined by the Policy Authority. The Policy Authority will also determine whether any specific Certification Authority is approved for interoperation.

Requests for interoperation must be directed in the first instance to the Issuing Authority, whose contact details are given in Section 1.5.1 above.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Re-Key of Certificates governed by this Certificate Policy is permitted.

Re-Key requests from Subscribers and any Participant shall at minimum, incorporate mechanisms for Authentication that fulfil initial Authentication requirements under this Certificate Policy. Proof of control of a valid Certificate as Authentication is permitted. Section 2 of the relevant PKI Disclosure Statement may introduce other permitted approaches to Authentication.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Re-Key, after Revocation requests to the Registration Authorities, must at a minimum include the identification and Authentication of the requester to at least the initial Authentication standards required under this Certificate Policy. This by definition is an issuance of a new Certificate.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests must at a minimum include the identification and Authentication of the requester and sufficient information to uniquely identify the Certificate to be Revoked. Valid proof of control of the Certificate to be Revoked is permitted as Authentication.

The risk of fraudulent misuse of the Private Key associated with the Certificate to be Revoked must be recognised. Where reliable Authentication of the Revocation request is not possible or is omitted, either the Issuing Authority, or Registration Authority acting on its behalf, is authorised to conduct Revocation. In such cases, the Issuing Authority or Registration Authority shall seek confirmation of the request to the greatest extent possible by practical means, prior to Revocation.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

Certificate applications may be made by:

- A Subscriber
- A Subject acting on behalf of a Subscriber
- A Registration Authority
- A Subject acting on behalf of a Registration Authority

Certificate applicants must comply with the procedures described in this Certificate Policy. Eligible Subscribers are specified in Section 15 of the relevant PKI Disclosure Statement.

An application for a Certificate does not oblige an Issuing Authority to Issue a Certificate.

4.1.2 ENROLMENT PROCESS AND RESPONSIBILITIES

A range of enrolment processes are permitted.

The Issuing Authority or Registration Authority in the Registration Authority Procedures defines the specific processes associated with a particular enrolment mechanism.

In all cases enrolment processes shall include:

- Provision of accurate information in support of Authentication (and validation of a Subject if applicable).
- Proof of control of the Private Key Pair by the Subject
- Acceptance of the Subscriber Agreement by the Subscriber.
- Agreement to comply with this Certificate Policy and obligations of Subscribers as defined in Section 4 of the relevant PKI Disclosure Statement and in the Subscriber Agreement.

4.1.2.1 REGISTRATION AUTHORITIES AND THEIR REPRESENTATIVES

Enrolment of Registration Authorities and their representatives is undertaken once the Registration Authority organisation has been approved by the Issuing Authority and contracted as an authorised Registration Authority.

Issuance of Certificates to Aviareto Registration Authority personnel shall be approved by the Issuing Authority. The relevant PKI Disclosure Agreement may provide for other Authorized Registration Authorities.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The Issuing Authority or an approved Registration Authority acting on its behalf is permitted to conduct Authentication of Subscribers and Subjects.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

The Issuing Authority or Registration Authority acting on its behalf will either approve or reject a Certificate application.

Where an application fails to achieve the specified Authentication requirements or the level of assurance of Authentication cannot be met, a Certificate application will be rejected.

Where a Certificate application is rejected, the reasons for rejection may be given to the applicant in accordance with the Registration Authority Procedures.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

No stipulation.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

Certificates shall be Issued automatically by the Certificate Authority only in response to a properly constructed, signed and validated Certificate request from the relevant Registration Authority. Only an approved Registration Authority can communicate with the associated Certificate Authority to submit a Certificate request.

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

The Certificate Manufacturer does not communicate with the Subscriber or Subject regarding Certificate Issuance. The Registration Authority is responsible for such notification where applicable.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

A Subscriber shall explicitly indicate acceptance of a Certificate to the Issuing Authority, or Registration Authority acting on its behalf. This may be via technical or procedural processes.

Collection of a Certificate via on line Authentication by the Subscriber or Subject constitutes acceptance of the Certificate.

Acceptance of tokens, smart cards or similar devices which Hold Private Keys constitutes acceptance of the associated Certificate.

Use of a Private Key for an activity or transaction approved under this Certificate Policy, or relevant PKI Disclosure Statement, constitutes acceptance of the associated Certificate.

The Issuing Authority shall ensure that the Subscriber (or its authorised representative), during application for or delivery of a Certificate, is provided with the details of terms and conditions stipulated in this Certificate Policy, the relevant PKI Disclosure Statement, the associated Subscriber Agreement and any other applicable contractual commitments.

The Subscriber (or its authorised representative) must acknowledge that it agrees to the terms and conditions stipulated in the Certificate Policy, the relevant PKI Disclosure Statement, the associated

Subscriber Agreement and any other applicable contractual commitments prior to first use of the Certificate.

For a Subject or device requesting and collecting a Certificate, the authorised representative of the Subscriber (which may be the Subject) may give this acknowledgement.

The Issuing Authority shall undertake to clearly inform the Subscriber that by accepting a Certificate Issued under this Certificate Policy, a Subscriber agrees to, and certifies, that at the time of Certificate acceptance and throughout the operational period of the Certificate, until notified otherwise by the Subscriber:

- No unauthorised person has ever had access to the Subscriber's Private Key or any related Activation Data.
- All information given by the Subscriber to the Issuing Authority or Registration Authority is true and accurate.

The above stipulations may be integrated with the Certificate application process as appropriate.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

The Certificate Manufacturer (or Certificate Authority) places the Issued Certificate in a Repository at the location specified by the Issuing Authority. The Repository may be subject to access restrictions.

Further "publication" of the Certificate is permitted. Details of approved Repositories are provided in Section 14 of the relevant PKI Disclosure Statement.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

The Certificate Manufacturer (or Certificate Authority) does not directly inform any other Participants of the Issuance of a Certificate.

Notification of Certificate Issuance by inclusion into a directory or other mechanism for Certificate Discovery is permitted.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscribers must ensure that use of the Private Key associated with the Certificate is consistent with the usage restrictions in the Certificate as stipulated and published by the Issuing Authority in the relevant PKI Disclosure Agreement.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

A Relying Party may only rely on a Subscriber's Public Key and Certificate for the specific functions stipulated and published by the Issuing Authority, or where PKIs interoperate, through the terms and conditions as stipulated and published in an interoperability agreement, or similarly named document.

Relying Parties must satisfy the requirements for reliance on a Certificate defined in Section 5 of the relevant PKI Disclosure Statement.

4.6 CERTIFICATE RENEWAL

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

Certificates may be Renewed at any time during their Operational Period. Renewal of Revoked or Suspended Certificates is not permitted. Renewal of Expired Certificates may be permitted as set out in the relevant PKI Disclosure Statement, but shall not be permitted in any case beyond 3 months from expiration.

Renewal requests from Subscribers and any other Participant shall at minimum, incorporate mechanisms for Authentication that fulfil initial Authentication requirements. Proof of control of a valid Certificate as Authentication is permitted.

Unless specifically and expressly approved by the Issuing Authority, Renewal shall incorporate Re-Key of the Certificate.

4.6.2 WHO MAY REQUEST RENEWAL

Renewal applications may be made by:

- A Subscriber holding the Certificate.
- A Subject acting on behalf of a Subscriber holding the Certificate.
- A representative of a Subscriber acting on behalf of the Subscriber holding the Certificate.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

The Issuing Authority or Registration Authority acting on its behalf will either approve or reject an application for Certificate Renewal.

Certificate Renewals are automatically processed by the Certificate Manufacturer (or Certificate Authority) in response to a properly constructed and signed Certificate request from the relevant Registration Authority.

Extension of validity of a Key Pair beyond the initial validity period of the Key Pair, as defined by the Operational Period of Certificate, is not permitted.

The relevant PKI Disclosure Statement may contain further terminology explanations.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

As specified in Section 4.3.2.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

As specified in Section 4.4.1.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

As specified in Section 4.4.2.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

As specified in Section 4.4.3.

4.7 CERTIFICATE RE-KEY

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

Re-Key of Certificates is permitted as specified in the relevant PKI Disclosure Statement. Re-Key of Revoked or Suspended Certificates is not permitted.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

Re-Key requests may be made by:

- A Subscriber holding the Certificate.
- A Subject acting on behalf of a Subscriber holding the Certificate.
- A representative of a Subscriber acting on behalf of the Subscriber holding the Certificate.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

The Issuing Authority or Registration Authority acting on its behalf will either approve or reject a request for Re-Key of a Certificate.

Certificate Re-Key requests are automatically processed by the Certificate Manufacturer (or Certificate Authority) in response to a properly constructed and signed Certificate request from the Issuing Authority or the relevant Registration Authority.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

As specified in Section 4.3.2.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Acceptance of a Re-Keyed Certificate is the same as that for Issued Certificates. See Section 4.4.1.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

As specified in Section 4.4.2.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

As specified in Section 4.4.3.

4.8 CERTIFICATE MODIFICATION

4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

Certificate modification is not permitted. Changes to Certificates must be enacted via issuance of a new Certificate or one of the approved processes specified in this Certificate Policy.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

See Section 4.8.1.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

See Section 4.8.1.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See Section 4.8.1.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

See Section 4.8.1.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

See Section 4.8.1.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See Section 4.8.1.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

Certificate Status Information shall identify all Revoked and/or Suspended Certificates; at least during the relevant Operational Period of a Certificate.

Upon Revocation or Suspension of a Subscriber's Certificate, the Issuing Authority shall undertake to inform the Subscriber.

4.9.1 CIRCUMSTANCES FOR REVOCATION

The circumstances under which Certificate Revocation may be requested (and carried out) are defined by the Issuing Authority and published as appropriate. The Registration Authority is responsible for the implementation of the decision of the Issuing Authority.

Registration Authorities must conduct verification of Revocation and Suspension Requests in accordance with this Certificate Policy. See Section 3.4.

A Certificate must be Revoked:

- When any of the information in the Certificate is known or suspected to be inaccurate.
- Upon suspected or known compromise of the Private Key associated with the Certificate.
- Upon suspected or known compromise of the media holding the Private Key associated with the Certificate.
- Upon suspected or known compromise of Activation Data.
- When the Subscriber (Subject) withdraws from or is no longer eligible to participate in the PKI governed by this Certificate Policy.

The Issuing Authority or Registration Authority acting on its behalf may Revoke a Certificate when a Subscriber or Subject fails to comply with obligations set out in this Certificate Policy, the relevant PKI Disclosure Statement, any additional published documents defining practices to be followed by the End-Entity, any other relevant agreement, or any applicable law or where revocation is required by relevant sanction and/or export control regulations.

4.9.2 WHO CAN REQUEST REVOCATION

The Revocation of a Certificate may be requested by any entity, provided they are Authenticated according to Section 3.4 of this Certificate Policy.

Revocation requests must present a valid circumstance for Revocation according to Section 4.9.1.

Approval of a Revocation request may only be granted by one of the following:

- The Policy Authority.
- The Issuing Authority.
- An approved Registration Authority.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

Revocation must be requested promptly after detection of a compromise or any other event giving cause for Revocation as specified in Section 4.9.1.

A Revocation request may be initiated in the following ways, in order of preference:

- Electronically by a digitally signed message, where available.
- By personal representation to the Issuing Authority or a Registration Authority.
- Electronically by a non-signed message.
- By telephone call to the Issuing Authority or a Registration Authority.

Certificate Revocation requests will be received by the Registration Authority which must:

- Conduct Authentication of the requestor.
- Validate the reason for the request.
- Ensure sufficient information to uniquely identify the Certificate which is the subject of the request.

The risk of fraudulent misuse of the Private Key associated with the Certificate to be Revoked must be recognised. Where reliable Authentication of the Revocation request is not possible or even omitted, either the Issuing Authority or Registration Authority acting on its behalf, is authorised to conduct Revocation. In such cases the Issuing Authority or Registration Authority shall seek confirmation of the request to the greatest extent possible by practical means, prior to Revocation. Processes may involve additional checking and information gathering to allow the Issuing Authority or its representative to achieve a satisfactory level of assurance of the validity of the request.

Certificate Revocations are automatically processed by the Certificate Manufacturer (or Certificate Authority) in response to a properly constructed and signed Revocation instruction from the relevant Registration Authority.

4.9.4 REVOCATION REQUEST GRACE PERIOD

None. If the Revocation request is approved, it must be reflected in the next scheduled publication of Certificate Status Information.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

The time to process a Certificate Revocation request is made up of two elements:

- The time for the Certificate Revocation request to be validated, approved and action taken by the Registration Authority. This time is not constrained but the Registration Authority must take all reasonable steps to conduct the Revocation procedure expeditiously.

- The time taken for the Certificate Manufacturer to respond to the authorised Certificate Revocation request. The Certificate Manufacturer must respond promptly to authorised Revocation requests.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

The mechanisms that a Relying Party may use (or where defined in Section 5 of the relevant PKI Disclosure Statement) in order to check the Certificate Status Information of the Certificate upon which they wish to rely, must be via a Certificate Revocation List or equivalent on-line protocol that permits authenticity and integrity of the Status Information to be verified. Revocation checking requirements shall be defined in the Relying Party Agreement and in Section 5 of the relevant PKI Disclosure Statement.

Supported Revocation status checking mechanisms must be defined in Section 17 of the relevant PKI Disclosure Statement.

4.9.7 CRL ISSUANCE FREQUENCY (IF APPLICABLE)

The frequency of CRL issuance is defined in Section 17 of the relevant PKI Disclosure Statement.

4.9.8 MAXIMUM LATENCY FOR CRLS (IF APPLICABLE)

No stipulation.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

The availability of on-line Certificate Status checking is published by the Issuing Authority in Section 17 of the relevant PKI Disclosure Statement.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

The requirements on Relying Parties to perform on-line Certificate Status checking are defined in Section 5 of the relevant PKI Disclosure Statement.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

The availability of other forms of Revocation advertisement is published by the Issuing Authority in accordance with Section 17 of the relevant PKI Disclosure Statement.

4.9.12 SPECIAL REQUIREMENTS RE KEY COMPROMISE

In the event of the compromise, or suspected compromise, of any Private Key, any Participant which is aware of same must notify the Issuing Authority or Registration Authority immediately and must indicate the nature and circumstances of the compromise, to the fullest extent known.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

This Certificate Policy does not support Suspension of Subscriber Certificates.

4.9.14 WHO CAN REQUEST SUSPENSION

See Section 4.9.13.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

See Section 4.9.13.

4.9.16 LIMITS ON SUSPENSION PERIOD

See Section 4.9.13.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

The types of Certificate Status checking services made available to the Subscriber by the Repository are defined in Section 17 of the relevant PKI Disclosure Statement.

4.10.2 SERVICE AVAILABILITY

The availability of any Certificate Status checking services that are available to Relying Parties is, if applicable, published in Section 17 of the relevant PKI Disclosure Statement.

4.10.3 OPTIONAL FEATURES

The optional features of any Certificate Status checking services that are available to the Relying Parties, if applicable, are published in Section 17 of the relevant PKI Disclosure Statement.

4.11 END OF SUBSCRIPTION

At the end of a commercial arrangement or subscription, the relevant Subscriber Certificates may either be Revoked or permitted to expire. The decision on which action to take is made by the Issuing Authority and implemented by the Registration Authority.

The actions to be taken in the event of the termination of the Trust Services will be defined in the contracts between the Issuing Authority, the Certificate Manufacturer and any other Participants providing the Trust Service.

4.12 KEY ESCROW AND RECOVERY

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

Participants providing Trust Services shall not offer or support any form of key escrow.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

This Certificate Policy does not prescribe or control session key management for applications.

Use of session key management is a matter for Subscribers.

The Issuing Authority does not offer or support any form of session key encapsulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Where “no stipulation” is stated in Section 5 of the Certificate Policy, it indicates there are no specific prescribed requirements for the controls, configuration or security requirements.

Where not stipulated, specific details on controls operated for components of the Trust Services must be detailed in the Certification Practice Statement and/or supporting documentation.

Controls must be approved by the Issuing Authority or auditors acting on its behalf.

5.1 PHYSICAL CONTROLS

5.1.1 SITE LOCATION AND CONSTRUCTION

Sites where Certificate Manufacturer or Time-stamping operations are carried out must:

- Satisfy at least the requirements specified by either ISO 27001, ETSI TS 319 401 or tScheme for CAs for production and control of Certificates.
- Be manually or electronically monitored for unauthorised intrusion at all times.
- Apply controls such that unescorted access to CAs or Time-stamping servers is limited to authorised personnel.
- Ensure unauthorised personnel are properly escorted and supervised.
- Ensure a site access log is maintained and inspected periodically.
- Ensure all removable media and paper containing sensitive plain text information is stored in secure containers.

Under this Certificate Policy, the detailed functionality of a Registration Authority may vary. In some scenarios, the Registration Authority is simply a data gatherer that assists the Issuing Authority in gathering registration or Revocation information from applicants, Authentication of applicants, and

forwarding the results to the Issuing Authority and/or Certificate Manufacturer. In other scenarios the Registration Authority may additionally initialise and load Certificates and Private Keys into protected stores or tokens. The physical security controls for the various types of Registration Authority will be different.

In the case where Registration Authorities act only as information verifiers/forwarders:

- Registration Authority sites must be located in areas that at least satisfy the controls required for the assurance levels for the level of registration and vetting conducted, and at a minimum be compliant with ISO 27001.
- If a Registration Authority is permitted to submit on-line requests for Certificate Issuance, the Issuing Authority will ensure the operation of the Registration Authority site provides appropriate security protection for any Registration Authority cryptographic modules, Registration Authority Private Keys, or other credentials supporting the process.
- A security container shall be utilised for storing any security devices and tokens used to gain access to Registration Authority functions.

In the case where the Registration Authority initialises and loads Certificates and Private Keys into stores or tokens, then the RA's physical security controls shall be equivalent to those required for Certificate Manufacturers as described in this Section. Subscriber key material shall not be stored on RA workstations.

All Repository sites must be located in areas that at a minimum satisfy the requirements for ISO 27001 and in addition, must:

- Ensure unescorted access to the Repository server is limited to authorised personnel.
- Ensure unauthorised personnel are properly escorted and supervised
- Ensure a site access log is maintained and inspected periodically.

Where Activation Data are recorded, they must be stored in a security container accessible only to authorised personnel.

5.1.2 PHYSICAL ACCESS

See Section 5.1.1.

5.1.3 POWER AND AIR CONDITIONING

No stipulation.

5.1.4 WATER EXPOSURES

No stipulation.

5.1.5 FIRE PREVENTION AND PROTECTION

No stipulation.

5.1.6 MEDIA STORAGE

Controls must be placed on all media used for the storage of information such as keys, Activation Data, confidential Subscriber information or CA information. Controls must be detailed in the Certification Practice Statement and/or supporting documentation.

5.1.7 WASTE DISPOSAL

All media used for the storage of information such as keys, Activation Data, confidential Subscriber information or CA files is to be sanitised or destroyed before released for disposal.

All documentation classified as confidential or equivalent shall be subject to a defined secure disposal procedure.

5.1.8 OFF-SITE BACKUP

Off-site backup arrangements must be in place as required by the business continuity arrangements outlined in Section 5.7.

Where data and facilities are removed from primary locations or in support of business continuity activities, controls must be applied which are at least comparable with those of the primary location.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

A Participant providing Trust Services must ensure a separation of duties for critical functions (Trusted Roles) to prevent a single person from compromising, maliciously using, or modifying PKI or supporting systems without detection.

The Certificate Manufacturer shall provide for the separation of distinct personnel roles by named personnel, distinguishing between day-to-day operation of the CA system and the management and audit of those operations. To the greatest extent possible, differing levels of physical and systems access control based on roles and responsibilities shall be employed to reflect the requirements of those roles and responsibilities. Controls must be detailed in the Certification Practice Statement and/or supporting documentation.

Registration Authorities must ensure that all Registration Authority personnel are adequately trained and understand their responsibility for the identification and Authentication of prospective Subscribers and related Certificate management tasks. Registration Authorities shall document arrangements for Trusted

Roles in the Registration Authority Procedures and/or supporting documentation. Arrangements must be approved by the Issuing Authority or auditors acting on its behalf.

A Registration Authority may permit all roles and duties for Registration Authority functions to be performed by one individual.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Multi-person control is required for CA Key generation.

Multi-person controls must be established for the performance of critical functions associated with the build and management of CA systems, including the software controlling Certificate Manufacturer operations.

All other duties associated with Certificate Manufacturer obligations, or with Participants providing other Trust Services, may be performed by an individual operating alone. However, verification processes employed must provide for oversight of all activities performed by Trusted Role holders.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

All Participants providing Trust Services shall ensure personnel in Trusted Roles are formally appointed and approved to hold the position. They shall have their identity and authorisation verified before they are:

- Included in the access list for the site of the Trust Service Provider.
- Included in the access list for physical access to the Trust Service Provider systems.
- Given a credential for the performance of their Trust Service Provider role.
- Given an access on Trust Service Provider systems.

Credentials issued to personnel in Trusted Roles must be:

- Managed so that their use can be detected and monitored.
- Managed so that their use is restricted to actions authorised for that role through applicable technical and procedural controls.
- Maintained under a prescribed and documented security policy.

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

For the Certificate Manufacturer, roles requiring the separation of duties are not specifically prescribed. The assignment of duties among personnel shall maintain appropriate separation of duties so as not to compromise the security arrangements for the Certificate Manufacturer procedures and other critical processes. The Certificate Manufacturer shall provide and maintain records of role allocation.

Other Participants providing Trust Services shall maintain appropriate separation of duties so as not to compromise the security arrangements for critical processes.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

A Participant providing Trust Services must ensure that all personnel performing duties with respect to its operation must:

- Be appointed in writing.
- Be bound by contract or statute to the terms and conditions of the position they are to fill.
- Have received training with respect to the duties they are to perform.
- Be bound by statute or contract not to disclose sensitive security-relevant information or Subscriber information and maintain required protection of personal information.
- Not be assigned duties that may cause a conflict of interest with their service provision duties.
- Not have been, as far as known, previously relieved of a past assignment for reasons of negligence or non-performance of duties.

Participants providing Trust Services may also specify additional criteria for security clearance of personnel, such as requirements for citizenship, rank, qualifications, satisfactory credit check, and absence of a criminal record. Any such additional requirements shall be stated in the Certification Practice Statement and/or supporting documentation.

5.3.2 BACKGROUND CHECK PROCEDURES

See Section 5.3.1.

5.3.3 TRAINING REQUIREMENTS

See Section 5.3.1.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

No stipulation.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

No stipulation.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

A Participant providing Trust Services must ensure that contractor access to its facilities is in accordance with this Certificate Policy. Individuals not security cleared must be under supervision by approved personnel at all times.

The actions of contracting staff are subject to the same audit arrangements and requirements as those of the personnel of the Participant providing Trust Services.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

All personnel associated with Trust Service provision shall be provided access to all documentation relevant to their position. This will include this Certificate Policy and associated Certification Practice Statements relevant to the service, together with any specific supporting documentation, statutes, policies or contracts relevant to the position and role of the personnel.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 TYPES OF EVENTS RECORDED

Certificate Manufacturer - Audit logs of all transactions relevant to Certificate creation, Certificate lifecycle management and the operation of Trusted Systems and services must be maintained to provide an audit trail. The event types are at a minimum:

- Messages received from authorised sources requesting an action on the part of the CA.
- All actions taken in response to requests.
- Trusted System installation and any modifications.
- Receipt, servicing and shipping of hardware cryptographic modules.
- Creation and issuance of CRLs.
- All error conditions and anomalies associated with the operation of Trusted Systems and services.
- Any known or suspected violations of physical security.
- Any known or suspected violations of network and/or Trusted System security.
- All CA and trusted application start-up and shutdown.
- All usage of the CA signing key.
- All personnel/role changes for Trusted Roles.

Registration Authority – must record for audit purposes, at a minimum the event types listed below:

- Any log on/off attempts by RA operators.
- All messages from authorised sources requesting an action of the RA and the subsequent actions taken by the RA in response to such requests.
- All messages to the CA requesting an action of the CA and the subsequent action taken by the CA.

- All physical accesses to RA systems (including components) and RA locations.
- RA application start-up and shut down.
- All use of any RA signing key(s).
- Any suspected or known violations of physical security.
- Any suspected or known violations of network and system security.
- All checks made for the registration of RA staff.
- All personnel/role changes for Trusted Roles.

5.4.2 FREQUENCY OF PROCESSING LOG

Participants providing Trust Services may review audit logs as appropriate to the items being recorded.

The Participant shall provide details of audit log processing in the records of role allocation in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or auditors acting on its behalf.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

Audit logs are to be retained for a period of no less than seven (7) years.

5.4.4 PROTECTION OF AUDIT LOG

The electronic audit log system must include mechanisms to protect the log files from unauthorised viewing, modification, and deletion. Manual audit information must be protected from unauthorised viewing, modification and destruction.

5.4.5 AUDIT LOG BACKUP PROCEDURES

Audit logs and audit summaries must be backed up or if in manual form, must be copied.

Such backups must be provided with the same level of security as the originals and must be commensurate with the data contained within them.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

No stipulation.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

No stipulation.

5.4.8 VULNERABILITY ASSESSMENTS

No stipulation.

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF RECORDS ARCHIVED

The event records and any accompanying data as described in Section 5.4.1 of this Certificate Policy are to be archived.

Participants providing Trust Services shall retain such additional information as may be required to ensure compliance with this Certificate Policy and/or legal requirements.

Registration Authorities must retain records of information provided in support of Certificate application and Revocation requests.

5.5.2 RETENTION PERIOD FOR ARCHIVE

Archived information is to be retained for a period of no less than seven (7) years

5.5.3 PROTECTION OF ARCHIVE

Archives are to be protected from unauthorised viewing, modification, and deletion. Archives are to be adequately protected from environmental threats such as temperature, humidity and magnetism.

Multiple copies of information may be archived.

5.5.4 ARCHIVE BACKUP PROCEDURES

No stipulation.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

No stipulation.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

No stipulation.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Participants providing Trust Services shall comply with the confidentially requirements specified in this Certificate Policy (see Section 9.3).

Records of individual transactions may be released to the requesting Participant upon request by a Participant involved in the transaction, or its recognised representatives.

Participants providing Trust Services shall ensure availability of their archives and that archived information is stored in a readable format during its retention period, even if the Trust Service Provider's

operations are interrupted, suspended or terminated. Appropriate disaster recovery and business continuity processes and procedures shall be maintained and implemented as necessary in accordance with Section 5.7.

In the event that the services of a Participant providing Trust Services for or on behalf of the Issuing Authority are to be interrupted, suspended or terminated, the Issuing Authority shall ensure the continued availability of the archive. All requests for access to such archived information shall be sent to the Issuing Authority or to the entity identified by the Issuing Authority prior to terminating its service.

5.6 KEY CHANGEOVER

Subscriber - a Subscriber may only renew or replace their Certificate and Key Pair prior to the expiration of the Key Pair, provided that the current Certificate remains valid and has not been Revoked or Suspended. This Key Pair changeover may be initiated by one of the following:

- The Subscriber (Subject).
- The Registration Authority.
- The Issuing Authority.

Automated notification of an impending required Key Pair changeover is permitted.

Subscribers without valid Key Pairs must be re-authenticated in the same manner as for an initial registration.

Where a Subscriber's Certificate has been Revoked as a result of suspected or actual non-compliance, the Registration Authority or the Issuing Authority that intends to initiate the Key Pair changeover process, must verify that the reasons for non-compliance have been satisfactorily addressed and resolved prior to Certificate Re-issuance.

All CA Certificates shall be made available in a Repository accessible to all Participants subject to Section 2.2 of the Certificate Policy.

All copies of old Issuing Authority Private Keys shall be:

- Destroyed such that the Private Keys cannot be retrieved; or
- Retained in a manner such that they are protected against being put back into use.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

A business continuity plan shall be in place to protect critical PKI processes from the effect of major compromises, failures or disasters. These shall enable the recovery of all Issuing Authority services. Business continuity and disaster recovery plans for Participants providing Trust Services shall be detailed

in the Certification Practice Statement and/or supporting documentation. Plans must be approved by the Issuing Authority or auditors acting on its behalf.

Participants providing Trust Services must provide evidence that such plans have been exercised.

In the case of compromise or suspected compromise of a Certificate Authority or Certificate Authority Keys, the Issuing Authority shall assess the impact of the compromise or suspected compromise and take action as appropriate. This could include:

- Notification to all Participants of the compromise.
- Revocation of Certificates.
- Publication of Certificate Status Information.
- Rebuild of the affected systems and the re-Issuance of Certificates.
- Other action as necessary, agreed between the Issuing Authority and impacted Participants.

The Policy Authority and/or Issuing Authority shall make any determination relating to Revocation of CA Certificates.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

Participants providing Trust Services must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. Business continuity plans for Participants providing Trust Services shall be detailed in the Certification Practice Statement and/or supporting documentation. Plans must be approved by the Issuing Authority or auditors acting on its behalf.

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

See Section 5.7.1.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

The business continuity plan for the Certificate Manufacturer shall be designed to deal with any disruption to the Trust Services and shall ensure managed, progressive recovery of components used to provide the Trust Services. A geographically separate alternative backup facility in order to maintain, at a minimum, for Certificate Status Information must be made available.

Any backup facility used for relocation following a disaster shall maintain compliance with this Certificate Policy. The provisions of this Certificate Policy shall be maintained during any relocation/transition.

Registration Authorities' deployment and configuration details vary. No specific business continuity requirements are defined. Registration Authority business continuity arrangements must be approved by the Issuing Authority or auditors acting on its behalf.

5.8 CA OR RA TERMINATION

The specific actions related to termination of the Trust Services, including all Certificate Manufacturer, Certificate Authority and Registration Authority functions shall be prescribed by the Issuing Authority. These could include, but may not be limited to:

- Informing both the Issuing Authority and Policy Authority for the governing Certificate Policy of the relevant termination.
- Provision of appropriate notice to all affected Participants.
- Revoking all relevant CA, RA and Subscriber Certificates.
- Ensuring all CA Private Keys are destroyed or put beyond use.
- Arranging with a third party for the preservation and storage of records for the minimum period of time stipulated for the service being terminated, but in any event not less than 7 years.

6 TECHNICAL SECURITY CONTROLS

Where “no stipulation” is stated in this section of the Certificate Policy it indicates there are no specific prescribed requirements for the controls, configuration or security requirements.

Specific details on technical controls operated for components of the Trust Services must be detailed in the Certification Practice Statement and/or supporting documentation. Controls must be approved by the Issuing Authority or auditors acting on its behalf.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

Certificate Manufacturer - CA Key Pairs and Issuing Authority Key Pairs shall be generated in a protected environment. Key Pair generation shall be multi-person control using random numbers of such length so as to make it computationally infeasible to regenerate them, even with the knowledge of the when and in which equipment they were generated. See Section 6.2.1.

Private Keys used in any Issuing Authority and/or Trust Services process that affects the outcome of Issued Certificates and Certificate Status Information services (such as signing of Certificate Revocation Lists), must be generated under controlled procedures. Participants conducting such key generation shall provide details of the procedure in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or auditors acting on its behalf.

Subscribers’ (Subjects’) Key Pairs may be generated by the Subscriber (Subject) or Registration Authorities approved by the Issuing Authority to conduct Key Pair generation. Procedures must be approved by the Issuing Authority or auditors acting on its behalf.

Private Keys used for signing shall only be generated by the Subscriber (Subject) or generated under the direct control of the Subscriber (Subject).

Where Key Pairs are generated by Registration Authorities, the generation procedure and storage of the Private Key shall prevent it from being exposed outside of the system that created it. Furthermore, it shall be erased from the system immediately after having been transferred to a security environment that is approved by the Issuing Authority and satisfies the requirements of Section 6.2.1.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

If the Private Key is not generated by the Subscriber, which in any case must only be accomplished, according to Section 6.1.1, it must be delivered to the Subscriber (or Subject) by the approved generator of the Private Key and satisfying the requirements of Section 6.2.1. In this case:

- The security environment containing the Private Key, protected with its initial Activation Data, shall be distributed to the Subscriber in a way that prevents it from being found together with the Activation Data, until it has been delivered to the Subscriber. This can be achieved by using separate channels of distribution for security environments and their associated Activation Data, or by clearly separating their distribution in time.
- The security environment issuer may supply the Activation Data delivering it directly to the Subscriber or Subject.
- Delivery of a security environment containing a Private Key that is (or will be) associated with a Certificate according to this Certificate Policy, is only allowed to be affected to the Subscriber in person through a face to face meeting with the Issuing Authority, or other authorised representative of the Issuing Authority. A sufficiently trusted representative of the Issuing Authority for this purpose would normally be the Registration Authority, but must be identified to the Subscriber at the time of application. To obtain the security environment, the Subscriber shall present valid identification that at least meets the requirements for initial registration (see Section 3.2). The means of identification must be recorded.
- Subscribers must acknowledge receipt of the security environment in writing which is retained by the Issuing Authority.
- Controls shall be in place to ensure the Subscriber shall replace initial Activation Data for the security environment with personally chosen Activation Data.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Certificate Manufacturer – All Public Keys from Registration Authorities shall be delivered in a secure manner using a standard, recognised protocol; (e.g. PKCS#10).

Registration Authority - The mechanism by which Subscriber Public Keys are delivered to the Certificate Manufacturer through the Registration Authorities is described in the Registration Authority Procedures.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The delivery of Public Keys to the Certificate Authority shall use PKCS#10 or other equivalent standards compliant cryptographic mechanism or using a process specifically approved by the Certificate Manufacturer. Specific mechanisms must be approved by the Issuing Authority.

6.1.5 KEY SIZES

The size of Issuing Authority and any supporting CA-Keys shall be not less than 2048 bit modulus for RSA.

The size of Subscribers' Private Keys shall be not less than 2048 bit modulus for RSA.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

Public Key exponents shall be of values and lengths that make known attacks (e.g. low exponent attacks) infeasible.

6.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

Certificates Issued under this Certificate Policy may be used only in applications and services as listed in Section 2 of the relevant PKI Disclosure Statement. A Certificate may be used for one or more of the following key usage services in connection with those applications and services:

- Digital signature.
- Non-repudiation[1].
- Key Encipherment.
- Data Encipherment.
- Key Agreement.
- Certificate Signature.
- CRL Signature.
- Encrypt only.
- Decrypt only.

Where a Certificate has been issued under this Certificate Policy for the purposes of Non–Repudiation, the Private Key shall be used solely for the purpose of Non-Repudiation.

Use of extensions in the Certificate shall be consistent with Section 7.1.2 of this Certificate Policy.

[1] This CP aligns with RFC 5280 and RFC 6818. ITU/ISO x.509 standards have modified this usage option to Content Commitment which may operate under modified usage terms. Any such usage terms shall be defined in Section 2 of the relevant PKI Disclosure Statement.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

CA-Keys shall be protected by high assurance physical and logical security controls. They must be stored in, and operated from inside, a specific tamper resistant hardware based security module that complies with FIPS140-2 level 3, its equivalents and successors.

Private Keys used in any Issuing Authority and/or Registration Authority process that affects the outcome of Issued Certificates and Certificate Status Information services (such as signing Certificate Revocation Lists), shall be protected by, maintained in, and restricted to, a hardware cryptographic token designed to meet the level of requirements as specified in FIPS 140-2 level 2, or its equivalents and successors.

CA-Keys shall not be available in unprotected form (complete or unencrypted) except in approved cryptographic modules.

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

For CA-Keys and Key Pairs that affect the outcome of Issued Certificates and Certificate Status Information services, at a minimum, two-person control is required.

6.2.3 PRIVATE KEY ESCROW

No stipulation.

6.2.4 PRIVATE KEY BACKUP

Participants providing Trust Services may back up and archive Private Keys, including CA-Keys.

In all cases, backups of Private Keys shall at a minimum be protected to the standards commensurate with that stipulated for the primary version of the Private Key as noted in Section 6.2.1 above.

In the case of aggregated backups of Private Keys, (for example, many Private Keys backed-up inside and protected by a single security environment), the backed-up Private Keys must be protected at a level commensurate with that stipulated for the Issuing Authority's Private Key.

6.2.5 PRIVATE KEY ARCHIVAL

No stipulation.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

If Subscriber Private Keys are not generated in the End-Entity's cryptographic module, it must be entered into the module via the use of a secure procedure approved by the Issuing Authority. Mechanisms to

protect Private Key material and any associated Activation Data from unauthorised access, modification and use shall be employed.

Participants conducting such Private Key transfer shall provide details of the procedure in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or auditors acting on its behalf. See Section 6.1.2.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

For CA-Keys, keys that affect the outcome of Issued Certificates, Certificate Status Information services and other business processes, prescribed standards are required for the cryptographic protection of Private Keys. See Section 6.2.1.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

Subscribers and Subjects who are natural persons must be authenticated to their cryptographic module before the activation of their Private Key. This Authentication may be in the form of a PIN, pass-phrase, password or other Activation Data. When deactivated, Private Keys must not be exposed in plaintext form.

Where Subjects are devices, software or hardware access controls shall be such that only authorised computer systems or services and/or authorised personnel may activate the Private Key.

Cryptographic modules used by Participants providing Trust Services which are used as components of Certificate lifecycle management shall block themselves after a specified number of consecutive failed attempts to authenticate to the module.

Cryptographic modules used by Participants providing Trust Services and security environments used by Subscribers may contain an unblocking function. Unblocking shall require the authorised personnel to use a mechanism to authenticate to the module.

Participants conducting unblocking must provide details of the procedure in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or auditors acting on its behalf.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

No stipulation.

6.2.10 METHOD OF DESTROYING PRIVATE KEY

Strict controls over destruction of CA-Keys and Key Pairs that affect the outcome of Issued Certificates and Certificate Status Information, must be exercised.

Whether active, expired or archived, the Issuing Authority must approve the destruction of such keys.

6.2.11 CRYPTOGRAPHIC MODULE RATING

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

Public Keys shall be archived in accordance with Section 5.5 of this Certificate Policy.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

Usage periods for Key Pairs shall be governed by validity periods set in Issued Certificates. These shall have the following maximum values:

- Subscribers – up to three (3) years.
- Trust Service Provider Trusted Roles – five (5) years.
- On-line intermediate Issuing Authorities – ten (10) years.
- Off-line primary Issuing Authorities – twenty (20) years.

Certified Private Keys shall not be extended beyond the initial lifetime of the Certificate Issued to Authenticate them. This means that a Renewal which would result in Certificate expiry after the expiry date for the original Certificate issued for that Key Pair is not permitted.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

All Issuing Authority supporting CA-Keys and Key Pairs that affect the outcome of Issued Certificates and Certificate Status Information services shall have Activation Data that is unique and unpredictable. The Activation Data, in conjunction with any other access control, must have an appropriate level of strength for the Key Pairs or data to be protected. Where PINs, passwords or pass-phrases are used, the relevant Participant must have the capability to change these at any time.

If applicable, unblocking code for a cryptographic module (if available) shall only be delivered to the legitimate holder of the module after an express request from the holder. Delivery of the unblocking code requires strong identification of the holder. See Section 6.2.8.

6.4.2 ACTIVATION DATA PROTECTION

All Issuing Authority supporting CA-Keys and Key Pairs that affect the outcome of Issued Certificates and Certificate Status Information services shall have mechanisms for the protection of Activation Data which is appropriate to the CA-Keys and Key Pairs being protected.

Details of protection shall be provided in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or auditors acting on its behalf.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

Participants providing Trust Services shall implement security measures that have been identified through a threat assessment exercise and must cover the following functionality where appropriate, including as specified in this Certificate Policy:

- Access control to the Trust Services and PKI roles.
- Enforced separation of duties for PKI roles.
- Identification and Authentication of PKI roles and associated identities.
- Use of cryptography for session communication and database security.
- Archive of Participant history and audit data.
- Audit of security related events.
- Trusted path for identification of PKI roles and associated identities.
- Recovery mechanisms for Key Pairs of Participants providing Trust Services.

This functionality may be provided by the operating system, or through a combination of operating system, Certificate Authority (CA) System, and physical safeguards.

Participants providing Trust Services shall document procedures in the Certification Practice Statement and/or supporting documentation. Procedures shall at a minimum include logging and audit requirements for processes related to initialisation, resetting, shutdown or reconfiguration of Certificate Authorities and any services that affect the outcome of Issued Certificates and Certificate Status Information.

6.5.2 COMPUTER SECURITY RATING

Participants providing Trust Services may use system components that do not possess a formal computer security rating provided that all requirements of this Certificate Policy are satisfied.

Any hardware security module or device holding CA Keys must comply with the requirements of Section 6.2.1 of this Certificate Policy.

Where specific computer security rating requirements are specified in this Certificate Policy, details of relevant components and how they satisfy the requirements must be provided in the Certification Practice Statement and/or supporting documentation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

The development of software that implements Trust Service functionality shall as a minimum be performed in a controlled environment that, together with at least one of the following approaches, shall protect against the insertion of malicious logic.

- The system developer shall have a quality system compliant with international standards or;
- The system developer shall have a quality system available for inspection and approval by the Issuing Authority.

6.6.2 SECURITY MANAGEMENT CONTROLS

The configuration of systems operated by Participants providing Trust Services as well as any modifications, upgrades and enhancements must be documented and controlled. There must be a method of detecting unauthorised modification or configuration of the software supporting Trust Services. Participants providing Trust Services shall ensure that it has a configuration management process in place to support the evolution of the systems under its control.

Details of security management systems shall be provided in the Certification Practice Statement and/or supporting documentation which must be approved by the Issuing Authority or auditors acting on its behalf.

6.6.3 LIFE CYCLE SECURITY CONTROLS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

Trust Service Provider systems must be protected from attack through any open or general-purpose network with which they are connected. Such protection must be provided and configured to allow only the minimal set of functions, protocols and commands required for the operation of the Trust Service.

Participants providing Trust Services shall detail the standards procedures and controls for network security in the Certification Practice Statement and/or supporting documentation which must be approved by the Issuing Authority or auditors acting on its behalf.

6.8 TIME-STAMPING

Time recording shall be implemented for all Certificate and other related activities that require recorded time. A synchronised and controlled time source shall be used.

Participants providing Trust Services shall detail the time source used and mechanisms for its control in the Certification Practice Statement and/or supporting documentation which must be approved by the Issuing Authority or auditors acting on its behalf.

7 CERTIFICATE, CRL, AND OCSP PROFILES

Certificates issued to (i) natural persons and natural persons associated with a legal person; and (ii) legal persons, shall comply with ETSI EN 319 412-2, and ETSI EN 319-412-3, respectively.

7.1 CERTIFICATE PROFILE

Certificate Profiles are under the direct control of the Issuing Authority.

Procedures for development of Certificate Profiles shall incorporate approval by the Issuing Authority prior to implementation.

7.1.1 VERSION NUMBER(S)

Only Certificates conformant to X.509 Version 3 and IETF RFC 5280 may be Issued.

7.1.2 CERTIFICATE EXTENSIONS

All End-Entity PKI software must correctly process the extensions identified in Sections 4.2.1 and 4.2.2 of the IETF RFC 5280 Certificate Profile Specification. The following are common Certificate extensions:

- The Basic Constraints extension is set to TRUE for CA-certificates only; its use is critical specifying that it is a CA-certificate. Subscriber End-Entity Certificates have the value set to FALSE.
- The Certificate Policies extension is mandatory and shall contain an OID indicating the use of this Certificate Policy (according to Section 7.1.6). The Certificate Policy Qualifier Info extension shall be used to direct End-Entities to where this Certificate Policy and other relevant information may be found.
- Where CRLs are used to produce Certificate Status information, the CRL distribution point extension is mandatory, and shall identify a location where the latest CRL Issued by the Issuing Authority can be obtained.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

No stipulation.

7.1.4 NAME FORMS

The use of all name forms shall be consistent with Section 3.1 of this Certificate Policy. Name forms shall be approved by the Issuing Authority.

7.1.5 NAME CONSTRAINTS

No stipulation.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

This Certificate Policy has been assigned an OID as defined in Section 12 of the relevant PKI Disclosure Statement. This shall be included in the Certificate Policy extension of all Certificates Issued under this Certificate Policy.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

No stipulation.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

No stipulation.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

No stipulation.

7.2 CRL PROFILE

7.2.1 VERSION NUMBER(S)

Only Certificate Revocation Lists conforming to X.509 version 2 and IETF RFC 5280 may be issued.

An alternative to CRLs may be permitted. The Issuing Authority may allow for provision of an on-line Certificate Status checking service, which meets the requirements in this Certificate Policy.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

No stipulation.

7.3 OCSP PROFILE

7.3.1 VERSION NUMBER(S)

OCSP and other forms of Certificate Status Information provision may be permitted.

Where permitted, Repositories shall detail the mechanisms for on-line Certificate Status Information provision in the Certification Practice Statement and/or supporting documentation which must be approved by the Issuing Authority or auditors acting on its behalf.

Mechanisms for on-line Certificate Status Checking shall be specified in Section 17 of the relevant PKI Disclosure Statement.

7.3.2 OCSP EXTENSIONS

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The details for assessment are specified in contractual arrangements between the Issuing Authority and the Participants providing Trust Services.

For all Participants providing Trust Services, audit must be sufficient to demonstrate to both the Issuing Authority and Policy Authority that the services comply with this Certificate Policy and any supporting policy documents applicable to their services.

For Certificate Manufacturers, assessment shall be against prescribed criteria defined by the Policy Authority.

For Certificate Manufacturers, audit shall be conducted not less than annually.

The Issuing Authority may exercise right to audit any Participants providing Trust Services at any time.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The suitability of assessors to perform assessment of the Issuing Authority and its associated Registration Authorities is decided by the Policy Authority.

Approved auditors are as defined in Section 11 of the relevant PKI Disclosure Statement and may include internal auditing resources of Participants, subject to the approval of the Policy Authority.

For Certificate Manufacturers, audits shall be conducted by a third-party approved auditor.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The acceptability of auditors is decided by the Policy Authority.

8.4 TOPICS COVERED BY ASSESSMENT

Audit is required to ensure a Participant providing Trust Services is operating in accordance with its Certification Practice Statement, this Certificate Policy, its contract with the Issuing Authority and any declared assurance or approval schemes under which Trust Services are operated.

Where the Participants providing Trust Services use any designated authorised agents in order to provide those Trust Services, the audit shall include the operations of such designated authorised agents.

Audit will address all aspects of Trust Service operations (whether they directly or indirectly influence compliance with the Certification Practice Statement) to ensure overall standards of operation are commensurate with this Certificate Policy.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

For compliance audits of Participants providing Trust Services, where significant exceptions or deficiencies are identified, the Issuing Authority will inform the Policy Authority and determine the action to be taken. A remedial action plan will be developed with input from the approved auditor. The Policy Authority has overall responsibility to ensure implementation of the action plan. If an immediate threat to the security or integrity of the Trust Services is identified a corrective action plan which may include suspension or termination of non-compliant services will be developed, approved by the Policy Authority and implemented by the Issuing Authority. For lesser exceptions or deficiencies, the Issuing Authority will determine the course of action to be taken.

8.6 COMMUNICATION OF RESULTS

Where compliance with third party assurance or approval schemes under which Trust Services are operated has been audited, approval status shall be made publicly available by the Participants providing Trust Services if required under the scheme.

In the event of identification of material non-compliance with this Certificate Policy, the Issuing Authority shall make available to Subscribers and Relying Parties details of action to be taken as a result of the deficiency and any remedial action required to be taken.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

The Issuing Authority may establish fees for the Issuance of Certificates. Where fees are charged, the fee schedule may be published for Subscribers (and Subjects) in Section 2 of the relevant PKI Disclosure Statement.

9.1.2 CERTIFICATE ACCESS FEES

The Issuing Authority shall establish any fees for access to Certificate and Certificate Status Information. Where fees are charged, the fee schedule shall be made available to Relying Parties.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

The Issuing Authority shall establish any fees for access to Certificate and Certificate Status Information. Where fees are charged, the fee schedule shall be made available to End-Entities.

9.1.4 FEES FOR OTHER SERVICES

The Repository shall not impose any fees on the availability or distribution of this Certificate Policy, or any document incorporated by reference in any Certificate Issued under this Certificate Policy.

Fees for services such as access to archived information are permitted subject to approval by the Issuing Authority. If such fees are charged, the fee schedule shall be published and available to all affected parties.

9.1.5 REFUND POLICY

Refunds are specified in the commercial arrangements between the Issuing Authority and Subscribers and in Section 9 of the relevant PKI Disclosure Statement.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

The Issuing Authority maintains adequate insurance coverage or alternative mechanisms to fulfil its obligation in relation to the Issuance of Certificates.

Insurance requirements for Participants providing Trust Services are specified in contractual arrangements between the Issuing Authority and Participants.

9.2.2 OTHER ASSETS

No stipulation.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

Neither the Policy Authority nor the Issuing Authority provides warranty coverage to End-Entities.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

The Issuing Authority and all Participants providing Trust Services shall classify personal, privacy related or corporate information as confidential. Such information shall not be released without the prior consent of the Subscriber, unless required otherwise by law.

All Private Keys and associated Activation Data used or otherwise handled by Participants operating under this Certificate Policy shall be kept confidential by Participants unless required otherwise by law. Identification information or other personal information appearing on Certificates is considered confidential.

Audit logs and records shall not be made available as a whole, except:

- As required by law
- As part of audit (in which case only to an approved auditor)
- For verification of audit logs (see Section 4.6.7). Only records of individual transactions may be released.

This information shall not be disclosed by the Certificate Manufacturer unless permitted in accordance with this Certificate Policy or as required by law.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

Certificate Status Information is not classified as confidential or as private. Corporate information appearing on Certificates is not considered confidential.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

The Issuing Authority carries overall responsibility to protect confidential information. Responsibility to maintain the confidentiality of information is devolved to all Participants via this Certificate Policy, their respective contracts with the Issuing Authority and applicable supporting documentation.

9.4 PRIVACY OF PERSONAL INFORMATION

Participants and all others using or accessing any personal data in connection with matters dealt with by this Certificate Policy shall comply with the General Data Protection Regulation, the Irish Data Protection Act 2018, and any other applicable legislation relating to data protection, and any equivalent legislation or regulations in any relevant jurisdiction. Unless specified by special agreement, in the course of accepting a Certificate, all Subscribers (Subjects) have agreed, where necessary, to allow their personal data submitted in the course of registration to be processed by and on behalf of the Issuing Authority and used as explained in the registration process, and have been given an opportunity to opt out of having their personal data used for some purposes. They have also agreed, where consent is necessary, to let certain personal data appear in publicly accessible directories and be communicated to others.

9.4.1 PRIVACY PLAN

All Participants shall comply with data protection and privacy legislation applicable in their jurisdiction and the privacy requirements of this Certificate Policy and applicable supporting documentation. The Privacy Policy applicable to this governing Certificate Policy together with any specific obligations and requirements are defined in Section 8 of the relevant PKI Disclosure Statement.

Privacy information shall be classified and treated as confidential. Where applicable, privacy information shall have such additional controls applied as required to comply with data protection and privacy legislation for the jurisdiction in which it is being processed.

9.4.2 INFORMATION TREATED AS PRIVATE

See Section 9.3.1.

9.4.3 INFORMATION NOT DEEMED PRIVATE

See Section 9.3.2.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

The Issuing Authority carries overall responsibility to protect privacy information. Responsibility to protect privacy information is devolved to all Participants via this Certificate Policy, their respective contract with the Issuing Authority and applicable supporting documentation.

Participants also carry responsibility to protect privacy information to comply with data protection and privacy legislation for the jurisdiction in which they operate.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

Where private information is being processed, notification to the data subject and other notifications and declarations on use must be given as required to comply with data protection and privacy legislation for the jurisdiction in which it is being processed. See Section 9.4.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

Information shall only be disclosed where required by due process of law and, subject to any duty of confidence, if it is necessary to provide such information and/or data in any legal enquiries or proceedings.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Information held by the Certificate Manufacturer may also be disclosed:

- On the owner's request, to facilitate such disclosure an Authenticated request from the information owner must be provided prior to the release of the information.
- At the specific request of the Policy Authority. In the case of confidential or privacy information, approval of the data subject shall, where necessary, be obtained prior to release.

9.5 INTELLECTUAL PROPERTY RIGHTS

All copyright and other intellectual property rights in this Certificate Policy (the 'Materials'), provided or made available by Entrust (Europe) Limited, shall remain the property of Entrust (Europe) Limited. Entrust (Europe) Limited grants the Issuing Authority and those Participants (including Certificate Manufacturers), Subscribers, Relying Parties and other parties operating under the governing Certificate Policy, a non-exclusive license to make use of the materials only for the purposes and in compliance with the terms of this Certificate Policy, relevant Certification Practice Statements and any applicable contracts. The Materials may only be used in conjunction with a Public Key Infrastructure in which Entrust (Europe) Limited is a Participant providing Trust Services.

Participants and other parties operating under this Certificate Policy shall ensure that all information supplied to other Participants does not infringe upon any third-party rights including intellectual property rights.

All Participants shall ensure that in using the Trust Services provided under this Certificate Policy, they will do nothing illegal or in infringement of any third party rights and in particular will ensure that any material that they supply or transmit is not illegal, libelous, and does not infringe any intellectual property right.

9.6 REPRESENTATIONS AND WARRANTIES

The only applicable representations and warranties are those as detailed in Section 6 of the relevant PKI Disclosure Statement.

9.7 DISCLAIMERS OF WARRANTIES

The Participants acknowledge and agree this Certificate Policy does not rely on any undertaking, promise, assurance, statement, representation, warranty or understanding (whether in writing or not) of any person (whether party to this Certificate Policy or not) relating to the subject matter of this Certificate Policy, other than as expressly set out in this Certificate Policy or incorporated between the Certificate Manufacturer and the Issuing Authority. All such undertakings, promises, assurances, statements, representations, warranties or understandings are expressly excluded to the greatest extent permitted by applicable law.

9.8 LIMITATIONS OF LIABILITY

By signing a Certificate containing a policy identifier which indicates the use of this Certificate Policy, an Issuing Authority certifies to all who reasonably rely on the information contained in the Certificate, that the information in the Certificate has been checked according to the procedures laid down in this Certificate Policy.

The Issuing Authority assumes no liability whatsoever in relation to the use of Certificates or associated Key Pairs Issued under this Certificate Policy other than as set out in this Certificate Policy, any relevant End-Entity agreements and the relevant PKI Disclosure Statement.

The Issuing Authority shall not be liable for any consequential, indirect or incidental damages, nor for any loss of business, loss of profit or loss of management time, whether foreseeable or unforeseeable, arising out of breach of any express or implied warranty, breach of contract, tort, misrepresentation, negligence, strict liability however arising, or in any other way arising from or in relation to the use of or reliance on, any Digital Certificate except only where required by applicable law.

Nothing in this Certificate Policy excludes or restricts a Participant's liability for death or personal injury resulting from negligence or the negligence of its employees, agents or contractors or liability arising from fraudulent misrepresentation.

The Issuing Authority excludes all liability of any kind in respect of any transaction into which an End-Entity may enter with any third party.

The Issuing Authority is not liable to End-Entities either in contract, tort (including negligence) or otherwise for the acts or omissions of other providers of telecommunications or Internet services (including domain name registration authorities) or for faults in or failures of their equipment.

Each provision of this Certificate Policy, excluding or limiting liability, operates separately. If any part is held by a court to be unreasonable or inapplicable, the other parts shall continue to apply.

The Issuing Authority limits any liability of any kind whatsoever for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated

with the Issuance, use of, or reliance upon Certificates or associated Key Pairs Issued under this Certificate Policy, in excess of that specified in Section 6 of the relevant PKI Disclosure Statement.

9.9 INDEMNITIES

Subscribers will immediately indemnify and keep indemnified the Issuing Authority from and against all costs, claims, demands, liabilities, expenses, damages or losses (including without limitation any direct or indirect consequential losses, loss of profit and loss of reputation, and all interest, penalties and legal and other professional costs and expenses) arising out of or in connection with:

- Use of Certificates and/or Key Pairs Issued under this Certificate Policy in a manner that is not in accordance with this Certificate Policy; and
- Subscribers' negligence, default or breach of this Certificate Policy in any other manner.

If the Subscriber(s) becomes aware that a third party may make a claim against, or notifies an intention to make a claim against, the Issuing Authority which may reasonably be considered as likely to give rise to a liability, the Subscriber(s) shall:

- As soon as reasonably practicable give written notice of that matter to the Issuing Authority specifying in reasonable detail the nature of the relevant claim;
- Not make any admission of liability, agreement or compromise in relation to the relevant claim without the prior written consent of the Issuing Authority (such consent not to be unreasonably conditioned, withheld or delayed); and
- Give the Issuing Authority and its professional advisers reasonable access to the premises and personnel of the Subscriber(s) and to any relevant assets, accounts, documents and records within the power or control of the Subscriber(s) so as to enable the Issuing Authority and its professional advisers to examine such premises, assets, accounts, documents and records, and to take copies at their own expense for the purpose of assessing the merits of the relevant claim.

9.10 TERM AND TERMINATION

9.10.1 TERM

This Certificate Policy is extant from the date of publication and shall remain in force until otherwise terminated in accordance with Section 9.10.2, replaced or withdrawn by notice provided by the Issuing Authority, or is explicitly identified to be terminated.

9.10.2 TERMINATION

Without prejudice to any other rights to which it may be entitled, the Issuing Authority may give notice in writing to the Subscriber(s) terminating their respective Subscriber Agreements with immediate effect if:

- The Subscriber(s) commits a material breach of any of the terms of this Certificate Policy or the Subscriber Agreement and (if such a breach is remediable) fails to remedy that breach within 30 days of being notified in writing of the breach;
- An order is made or a resolution is passed for the winding up of the Subscriber(s) or circumstances arise which entitle a court of competent jurisdiction to make a winding-up order of the Subscriber(s)
- An order is made for the appointment of an administrator to manage the affairs, business and property of the Subscriber(s) or documents are filed with a court of competent jurisdiction for the appointment of an administrator of the Subscriber(s) or notice of intention to appoint an administrator is given by the Subscriber(s) or its directors or by a qualifying floating charge holder);
- A receiver is appointed of any of the Subscriber(s) assets or undertaking or if circumstances arise which entitle a court of competent jurisdiction or a creditor to appoint a receiver or manager of the Subscriber(s) or if any other person takes possession of or sells the other party's assets;
- The Subscriber makes any arrangement or composition with its creditors or makes an application to a court of competent jurisdiction for the protection of its creditors in any way;
- The Subscriber(s) ceases to trade or threatens to cease trade;
- There is a change of control of the Subscriber(s);
- The Subscriber(s) takes or suffers any similar or analogous action in any jurisdiction in consequence of debt.

Should this Certificate Policy be terminated prior to all extant Certificate Authorities, Issued Certificates shall be Revoked as part of the termination procedure (see Section 5.8).

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this Certificate Policy, the Participants are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates and this Section 9.10.3 shall survive termination.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 PARTICIPANTS (OTHER THAN THE ISSUING AUTHORITY)

Whenever any Participant hereto desires or is required to give any notice, demand, or request with respect to this Certificate Policy, such communication shall be made either by using digitally signed messages consistent with the requirements of this Certificate Policy, or by paper-based communications. Electronic communications shall be effective upon the sender receiving a valid, digitally signed acknowledgment of receipt from recipient. Such acknowledgement must be received within five working (5) days, or else notice must then be given by paper-based communications. Such paper-based communications must be delivered by a service that confirms delivery in writing or via certified or registered mail, postage prepaid, addressed to the Issuing Authority as detailed in Section 1 of the

relevant PKI Disclosure Statement under Issuing Authority. All such communications shall be effective upon receipt including as against the addressee of the communication.

A Participant requiring receipt of notice under this Certificate Policy is required to provide notice of:

- Changes in address including postal and e-mail addresses
- Changes in financial or other status, which would change the basis upon which the Certificate has been granted
- Any other notice pertinent to the maintenance of the provisions of this Certificate Policy.

9.11.2 ISSUING AUTHORITY

All notices by the Issuing Authority (irrespective of the capacity in which it is issuing the notice) shall be provided by digitally signed or unsigned messages, or by making such notice accessible online in a similar manner as that used for the publication of this Certificate Policy.

Notice requirements with regard to termination of Issuing Authority operations are specified in Section 5.8.

Notice requirements with regard to changes in this Certificate Policy are specified in Section 9.12.2.

9.11.3 NOTIFICATION

Any notices given pursuant to Section 9.11.2 shall be deemed served effective upon dispatch.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

Amendments to this Certificate Policy fall into three categories:

- Editorial or typographical corrections, or changes to the contact details which may be made without notification or awaiting comments.
- Changes which, in the judgement of the Policy Authority, will not materially impact a substantial majority of the End-Entities.
- Changes which, in the judgement of the Policy Authority, are likely to have a material impact upon a significant number of End-Entities.

Where the amendments are likely to have a major impact on the majority of End-Entities then it must be replaced by a new document (ref. Section 9.12.3).

9.12.2 NOTIFICATION MECHANISM AND PERIOD

All proposed changes that may materially impact End-Entities will be notified in accordance with Section 9.11 of this Certificate Policy by the Issuing Authority registered with the Policy Authority, and will be prominently posted on the World Wide Web site of the Issuing Authority which shall ensure that notice

of such proposed changes is posted in the Repository and shall make commercially reasonable efforts to advise End-Entities of such proposed changes.

Impacted Participants may file comments through the relevant Issuing Authority or directly with the Policy Authority, the period for comment will be as follows:

- For changes which, in the judgement of the Policy Authority, will not materially impact a substantial majority of End-Entities, comments shall be received within 5 days of original notice.
- Changes which, in the judgement of the Policy Authority, are likely to have a material impact upon a significant number of End-Entities, comments shall be received within 15 days of original notice.

Any action taken as a result of comments filed in accordance with the above is wholly at the discretion of the Policy Authority.

If the proposed change is modified as a result of comments received, notice of the modified proposed change shall be given at least 30 days prior to the change taking effect.

Approval for incorporation of any changes to this Certificate Policy is wholly at the discretion of the Policy Authority.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

If amendments to this Certificate Policy are determined by the Policy Authority to be sufficiently significant, the Policy Authority reserves the right to assign a new Object Identifier (OID) to the modified Certificate Policy.

9.13 DISPUTE RESOLUTION PROVISIONS

The Issuing Authority shall deal with such disputes in accordance with its dispute resolution process specified in Section 10 of the relevant PKI Disclosure Statement.

9.14 GOVERNING LAW

This Certificate Policy shall be governed by the law of Ireland and the parties submit to the exclusive jurisdiction of the courts of Ireland. In the event of any dispute (other than one relating to the infringement of intellectual property rights, for which an injunction would be the appropriate remedy) arising from or concerning this Certificate Policy, then such matter shall be settled between the parties according to Section 9.13.

9.15 COMPLIANCE WITH APPLICABLE LAW

All Participants will comply with all applicable law and regulations, for example those relating to cryptographic hardware and software that may be subject to the export control laws of a given jurisdiction.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

The Participants acknowledge that, except for documents expressly referred to or incorporated by reference herein, this Certificate Policy constitutes the entire agreement and understanding of the Participants and supersedes any previous agreement (save to the extent referenced herein) between the Participants (or any of them) relating to the subject matter of this Certificate Policy. For the purposes of this clause, such documents shall include, with regard to the End-Entities:

- The relevant PKI Disclosure Statement
- The Relying Party Agreement (as relevant)
- The Subscriber Agreement (as relevant)
- The Glossary of Terms

In the event of any ambiguity, inconsistent or incompatible provisions, this Certificate Policy shall take precedence, followed by the provisions of the relevant PKI Disclosure Statement, then Subscriber Agreement, then Relying Party Agreement.

9.16.2 ASSIGNMENT

This Certificate Policy shall be binding upon, and inure to the benefit of all Participants. The rights and obligations detailed in this Certificate Policy are not assignable by the Participants and any purported assignment without such consent shall be void.

9.16.3 SEVERABILITY

In the event that any one or more of the provisions of this Certificate Policy shall for any reason be held to be invalid, illegal, or unenforceable at law, such unenforceability shall not affect any other provision, but this Certificate Policy shall then be construed as if such unenforceable provision or provisions had never been contained herein, and insofar as possible, construed to maintain the original intent of the Certificate Policy.

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

No delay, neglect or forbearance on the part of one Participant in enforcing against any other Participant any term or condition of this Certificate Policy shall either be or be deemed to be a waiver or in any way prejudice any right of that Participant under this Certificate Policy. No right, power or remedy

in this Certificate Policy conferred upon or reserved for a Participant is exclusive of any other right, power or remedy available to that Participant. Each Participant shall bear its own legal costs and other costs and expenses arising out of or in connection with this Certificate Policy.

9.16.5 FORCE MAJEURE

The Issuing Authority shall have no liability to the Participants under this Certificate Policy if it is prevented from or delayed in performing its obligations under this Certificate Policy or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control, as set out in any relevant End-Entity agreements and the relevant PKI Disclosure Statement.

If any force majeure affecting the availability of or access by a Relying Party to Certificate Status Information continues for a continuous period of more than 72 hours, the Issuing Authority may terminate this Certificate Policy by written notice to the other Participants.

9.17 OTHER PROVISIONS

9.17.1 CERTIFICATE POLICY CONTENT

Section and paragraph headings shall not affect the interpretation of this Certificate Policy and the content of Section 1.3 is descriptive only for reference purposes and such section shall be interpreted accordingly.

9.17.2 THIRD PARTY RIGHTS

Save as expressly provided for below, no term of this Certificate Policy shall be enforceable by any third party. The parties who have direct rights are the Participants.

APPENDIX 1 - GLOSSARY

Terms used in this Certificate Policy are defined in the Glossary of Terms as set out below.

Activation Data	Private data, other than Keys, that are required to access cryptographic modules, including information such as passwords, passphrases, PINs, Private Keys or other shared secrets.
Asymmetric Cryptosystem	A system which generates and employs a secure key consisting of a Private Key for creating a Digital Signature and a Public Key to verify a Digital Signature. Also known as Public Key Cryptography.
Authentication	The process of establishing that individuals, organisations, or devices are who or what they claim to be. In the context of a PKI, Authentication can be the process of establishing that an individual or organisation applying for or seeking access to something under a certain name is, in fact, the proper individual or organisation. Authentication can also refer to a security service that provides assurances that individuals, organisations, or things are who or what they claim to be or that a Message or other data originated from a specific individual, organisation, or device. Thus, a Digital Signature of a Message Authenticates the Message's sender.
Certificate	A collection of data that at a minimum: 1. Identifies the Issuing Authority 2. Names or identifies its Subject 3. Contains the Subject's Public Key 4. Identifies the Operational Period of Certificate 5. Bears the Digital Signature of the Issuing Authority Also known as Digital Certificate.
Certificate Authority (CA) System	The software and hardware system used by the Issuing Authority or its designated Certificate Manufacturer to issue and manage the full lifecycle of Certificates.
Certificate Authority Certificate	See Issuing Authority Certificate.

(CA-Certificate)	
Certificate Authority Key (CA-Key)	The Private Key used by the Issuing Authority for signing Certificates and other objects.
Certificate Discovery	The process of obtaining a Subscriber's Certificate. Typically from a directory or database.
Certificate Manufacturer	The entity providing Certificate management services and facilities for an Issuing Authority.
Certificate Policy (CP)	A named set of rules that indicate the applicability of a Certificate to a particular community and/or class of application with common security requirements. A Certificate Policy may be employed by a Relying Party to help in deciding whether a Certificate (and the binding therein), is sufficiently trustworthy for a particular purpose. A CP may be supported by one or more Certification Practice Statements.
Certificate Profile	Defines the usage of the Certificate and is formally approved by the Policy Authority and the Issuing Authority.
Certificate Revocation List (CRL)	A list maintained by, or on behalf of, an Issuing Authority of the Certificates that it has issued, that have been Revoked or Suspended before the expiry stated in the Certificate.
Certificate Status Checking	The process of ascertaining the Certificate Status Information of a Certificate. Typically via a controlled mechanism from a Repository. Also known as Certificate Status Discovery.
Certificate Status Information	Information that indicates whether Certificates have been Revoked or Suspended; commonly provided via Certificate Revocation Lists, or individually through specific online enquiries (e.g. OCSP).
Certificate Service Provider (CSP)	See also Participant. Also known as a Trust Service Provider. The term CSP is used in connection with the EU Electronic Identification and Trust Services Regulation and supporting ETSI Standards.

Certificate User	See Relying Party.
Certificate Authority	See Issuing Authority.
Certification Path	A logical and ordered sequence of Certificates which, together with the Public Key of the initial object in the Certification Path, can be processed to obtain that of the final object in the Certification Path.
Certification Practice Statement (CPS)	A statement of the procedures and practices employed in the issuing, managing, revoking, and renewing of Certificates. A CPS may support one or more Certificate Policies.
Confirm	Ascertain through appropriate inquiry and investigation.
Content Commitment	An action whereby a Signer of a message commits to the content being signed by them. This term is sometimes used synonymously with Non-Repudiation; however, in any specific context the detailed definition may result in its legal standing differing from that of Non-Repudiation. See also Non-Repudiation.
Corresponding Private Key Corresponding Public Key	Given a Public Key taken from a Key Pair, the corresponding Private Key is the Private Key from that same Key Pair, (and vice-versa for Corresponding Public Key).
Cross-certificate	A Certificate used to establish a trust relationship between two Issuing Authorities.
Digital Certificate	See Certificate.
Digital Signature	The result of a transformation of a Message by means of a cryptographic system and a Hash Function, using Key Pairs such that a person who has the initial Message can determine: 1. Whether the transformation was created using the Private Key that corresponds to the Signer's Public Key, and 2. Whether the initial Message has been altered since the transformation was made.

End-Entity	Those using Digital Certificates. See Subscriber and Relying Party .
Hash Function	An algorithm mapping or translating one sequence of bits into another, generally smaller, set (the Hash or Message Digest) such that: 1. A Message yields the same Hash result every time the algorithm is executed using the same Message as input; 2. It is computationally infeasible that a Message can be derived or reconstituted from the Hash result provided by the algorithm; and 3. It is computationally infeasible that two Messages can be found that produce the same hash result using the algorithm.
Hash	The output produced by a Hash Function upon processing a Message (see also Message Digest).
High Security Zone	An area to which access is controlled through an entry point and is limited to authorised, appropriately screened personnel and properly escorted visitors. High Security Zones should be accessible only from Security Zones, and are separated from Security Zones and Operations Zones by a perimeter built to the specifications recommended in a threat risk assessment. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.
Hold a Private Key	To use or to be able to use a Private Key.
Incorporate by Reference	Make one Message a part of another Message by:- 1. Identifying the Message to be incorporated; 2. Providing information which enables the receiving party to access and obtain the incorporated Message in its entirety; and 3. Expressing the intention that it be part of the incorporating Message. The incorporated Message shall have the same effect as if it had been fully stated in the incorporating Message to the extent permitted by law.

Issuance (Issue a Certificate)	The acts of an Issuing Authority in creating a Certificate which is bound to a Subscriber. The process requires Authentication of the Subscriber and/or Subject.
Issuing Authority	By definition, an Issuing Authority is the entity listed in the issuer field of a Digital Certificate. The Issuing Authority may obtain benefit in return for taking on the risks associated with transactions secured by Digital Certificates, for example, risk of fraud. The Issuing Authority has the responsibility for deciding who may be issued with a Certificate carrying its name.
Issuing Authority Certificate	A Certificate for an Issuing Authority's Public Key, and for use in signing Certificates created by certificate authority software under its control.
Key Pair	In an Asymmetric Cryptosystem - a Private Key and its mathematically related Public Key having the property that the Public Key can verify a Digital Signature that the Private Key creates.
Local Registration Authority (LRA)	See Registration Authority.
Message	A digital representation of information.
Message Digest	The output produced by a Hash Function upon processing a Message. See also Hash.
Message Integrity	The assurance of the unaltered status of a Message.
Non-Repudiation	Strong and substantial evidence of the identity of the Signer of a Message and of Message Integrity, sufficient to prevent a party from successfully denying the original submission or delivery of the Message and the Message Integrity. See also Content Commitment.
Notify	Communicate or make available information to another person as required under the circumstances.
Online Certificate Status Protocol (OCSP)	A network protocol used to ascertain the current validity status of a Certificate.
Operational Period of Certificate	The Operational Period of a Certificate begins on the date and time it is issued by an Issuing Authority (or on a later date and time if stated in the Certificate), and ends

	at the completion of its Validity Period unless it is earlier Revoked or Suspended.
Participant	An individual or organisation that plays a role within a given PKI, typically as a Subscriber, Relying Party, CA, RA or Certificate Manufacturer. Participants other than Subscribers, Subjects and Relying Parties (i.e. not End-Entities) may also be known as a Trust Service Provider (TSP) or a Certificate Service Provider (CSP).
Public Key Infrastructure (PKI)	A system of Digital Certificates, Certificate Authorities, and other components that verify and authenticate the validity of parties involved in electronic transactions.
PKI Disclosure Statement (PDS)	An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing, summarising and emphasizing information normally covered in detail by associated CP and/or CPS documents. A PDS is not intended to replace a CP or CPS.
Policy Authority	The entity that has ultimate responsibility for governance and control over the issuance, management and usage of a specified set of Digital Certificates. It uses a Certificate Policy as the mechanism to exercise control over all Participants in a PKI. Also known as Policy Management Authority (PMA).
Policy Qualifier	Policy dependent information that may accompany a CP identifier in an X.509 certificate.
Private Key	The private part of an asymmetric Key Pair used for public key encryption techniques. The Private Key is typically used for signing Digital Signatures or for decrypting Messages.
Public Key	The public part of an asymmetric Key Pair used for public key encryption techniques. The Public Key is typically used for verifying Digital Signatures or to encrypt Messages to the owner of the Private Key.

Public Key Cryptography	See Asymmetric Cryptosystem.
Registration Authority (RA)	An entity that is authorised or licensed by an Issuing Authority to carry out the practices and procedures for one or more of the following functions: 1. the identification and Authentication of Certificate applicants; 2. the approval or rejection of Certificate applications; 3. initiating Revocations or Suspensions under certain circumstances; 4. processing requests for Revocation or Suspension of Certificates; 5. approving or rejecting requests by for the Renewal or Re-Key of Certificates. 6. Process refunds where applicable An RA does not have responsibility for signing or issuing Certificates or Certificate Status Information.
Registration Authority Operator (RAO)	Registration Authority staff member with approvals to conduct a full set of Certificate management functions.
Relying Party	A recipient of a Certificate who acts in reliance on that Certificate and/or any Digital Signatures verified using that Certificate and as extended by the relevant PKI Relying Party Agreement.
Relying Party Agreement (RPA)	An agreement between an Issuing Authority and a Relying Party that typically establishes the rights and obligations between those parties regarding the verification of Digital Signatures or other uses of Certificates. Also known as Relying Party Charter.
Repository	The entity providing community-wide accessible mechanisms by which Participants can obtain Certificates or Certificate Status information to validate Certificates, and obtain Certificate Policy and other controlling information for the PKI.
Re-Key a Certificate	The process by which an existing Certificate has its Public Key value changed by issuing a new Certificate with a different (usually new) Public Key.

	Notably all characteristics relating to the Subject of the Certificate remain unchanged unless Re-Key is combined with a Renewal or Issuance of a new Certificate.
Renewal (Renew a Certificate)	The process by which an existing Certificate that is bound to a Subscriber is replaced by issuing a new Certificate to that Subscriber. Typically this is based upon the validity of the existing Certificate. This process normally involves a Re-Key.
Revocation (Revoke a Certificate)	Permanently end the Operational Period of Certificate from a specified time.
Revocation Information Suspension Information	Information required before enacting a Certificate Revocation (or Suspension, as relevant). It must include evidence of the authenticity of the requestor.
Signer	A person who creates a Digital Signature for a Message.
Subject	The individual, corporate entity, organisation or device named or identified in a certificate issued to a Subscriber, and who Holds a Private Key corresponding to the Public Key listed in the Certificate. A Subject may also be a Subscriber. A Subject must always be either: 1. a Subscriber or an individual acting on behalf of a Subscriber; or 2. formally bound under the jurisdiction and control of a Subscriber.
Subscriber	A person, corporate entity or organisation that contracts with an Issuing Authority for the issuance of Certificates. The Subscriber bears ultimate responsibility for the use of the Private Key associated with the Certificate. The Subscriber may be a Subject acting on their own behalf.
Subscriber Agreement	An agreement between an Issuing Authority and a Subscriber (or a Subject authorised to act for a Subscriber) that establishes the rights and responsibilities of the parties regarding the issuance and management of Certificates and associated Private Keys.
Suspension (Suspend a Certificate)	Temporarily make a Certificate non-operational by suspending the Operational Period of Certificate from a

	specified time for a period up to the end of its Validity Period.
Time-stamp Time-stamping	To create a notation that indicates, at a minimum, the correct date and time of an action or activity and the identity of the Participant that created the notation; or such a notation as is appended, attached or referenced as a part of a data structure. Time-stamps may, but do not require derivation of chronological data from a secure time source and/or use cryptographic techniques to preserve the integrity of the Time-stamp.
Time-stamping Authority	The Trust Service Provider operating, controlling and issuing Time-stamps for use by other entities.
Trusted Role	A function in the operation of a Trust Service, CA, RA or PKI that: 1. Can influence the status of issued Digital Certificates. 2. Is able to affect the security or functionality of components that enforce security of the Trust Service.
Trust Infrastructure	See Public Key Infrastructure.
Trust Service	1. A trust-enhancing service offered or performed by a Trust Service Provider that supports the assurance, integrity or security of electronically executed activities, (e.g. Time-stamping, notarisation, watermarking, etc.) 2. The service offered or performed by an Issuing Authority, Registration Authority, Certificate Manufacturer or other trusted intermediary relating to the issuance and control of Digital Certificates, (e.g. manufacture, Issuance, Revocation, publication, registration, validity-checking or defining policy).
Trust Service Provider (TSP)	An entity that acts as a supplier of Trust Services. Also known as Certificate Service Provider (CSP).
Trusted System	Computer hardware, software and procedures that: 1. Are adequately secure from intrusion and misuse;

	2. Provide an adequate level of availability, reliability and correctness of operation; 3. Are adequately suited to performing their intended functions; and 4. Adhere to generally accepted security principles.
Validation	See Authentication.
Validity Period	The period that is defined within a Certificate, during which that Certificate is intended to be valid. See also Operational Period of Certificate.
Verify (a Digital Signature and/or Message Integrity)	In relation to a given Digital Signature, Message and Public Key, to determine accurately: 1. That the Digital Signature was created during the Operational Period of Certificate by the Private Key corresponding to the Public Key listed in the Certificate; and 2. That the Message has not been altered since its Digital Signature was created.
Vettor	Registration Authority staff member with approvals to conduct a limited set of Certificate management functions.