REGISTERS OF SCOTLAND PKI-DRS BASE CERTIFICATE POLICY

Release	Date	Comment
1.0	08/2007	Initial publication to website.
2.0	07/2021	Updated text from Entrust. Republished to website.
2.1	07/2026	Updated URL. Republished to website.

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 various terms used throughout this document are explained in the Registers of Scotland (RoS) PKI-DRS Glossary of Terms at https://www.ros.gov.uk/services/digital-discharge-service/dds-for-lenders.

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 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. A PKI Disclosure Statement supporting this Certificate Policy incorporates this Certificate Policy by reference.

This Certificate Policy defines a Public Key Infrastructure and in conjunction with the PKI-DRS 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

This Certificate Policy has not been assigned an OID.

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
    - 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 the End-Entity relationship is with the Issuing Authority.

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. These descriptions 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 synonymous with Issuing Authority described in 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 a document known as the PKI Disclosure Statement. These provisions typically include, but are not limited to the following:

1. Policy Authority & Issuing Authority Contact Information
2. Certificate Type, validation procedures and usage
3. Reliance Limits
4. Obligations of Subscribers
5. Certificate Status checking obligations of Relying Parties
6. Limited Warranty & Disclaimer/Limitation of Liability
7. Applicable Agreements, Certification Practice Statement, Certificate Policy
8. Privacy Policy
9. Refund Policy
10. Applicable Law & Dispute Resolution
11. CA and Repository Trust Marks and Audit
12. Identification of the Certificate Policy
13. Approved Registration Authorities
14. Approved Repositories
15. Eligible Subscribers
16. Eligible Relying Parties
17. Certificate Status Information

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, 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 Policy and 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 PKI-DRS 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 are identified in section 15 of the PKI-DRS PKI Disclosure Statement.

1.3.4 SUBJECTS

Certificate issue to Subjects is not supported as part of the PKI governed by this Certificate Policy.

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 Relying-Parties for Certificates Issued under this Certificate Policy are specified in Section 16 of the PKI-DRS 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. Simply stated, 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 is identified in Section 1 of the PKI-DRS PKI Disclosure Statement.

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 by which primarily Subscribers and Relying Parties can obtain and validate information on Certificates Issued under this Certificate Policy.

The Issuing Authority has approved the Repositories identified in section 14 of the PKI-DRS PKI Disclosure Statement 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.

1.4.1.1 APPROPRIATE CERTIFICATE USES

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

1.4.1.2 PROHIBITED CERTIFICATE USES

All other application use and any other usage categories for Certificates Issued under this Certificate Policy is prohibited as described in Section 2 of the PKI-DRS PKI Disclosure Statement.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANISATION ADMINISTERING THE DOCUMENT

The Policy Authority, responsible for approving rights, obligations, liabilities and all other terms and conditions contained in this Certificate Policy is listed in Section 1 of the PKI-DRS PKI Disclosure Statement.

Entrust (Europe) Limited is authorised by the Policy Authority to administer this Certificate Policy. Entrust (Europe) Limited may be contacted as follows:

Entrust (Europe) Limited.
Building 273
Greenham Business Park
Thatcham,
Berkshire, RG19 6HN
UK

Email: info@trustis.com
Web: http://www.trustis.com

Tel: +44 (0) 1635 231361
Fax: +44 (0) 1635 231366

1.5.2 CONTACT PERSON

In the first instance, the Issuing Authority should be contacted regarding the contents of this Certificate Policy.

Contact details are provided in Section 1 of the PKI-DRS PKI Disclosure Statement.

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 of the PKI-DRS PKI Disclosure Statement.

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 PKI-DRS Glossary of Terms at https://www.ros.gov.uk/services/digital-discharge-service/dds-for-lenders.

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 it 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 of this PKI via the Repository:

- This Certificate Policy with its associated PKI Disclosure Statement.
- Any supporting policy documents and agreements.
- The Information that will allow the authenticity of the Certificate of the Issuing Authority's 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).
- Certificate Status Information for Certificates Issued under this Certificate Policy.

2.3 TIME OR FREQUENCY OF PUBLICATION

Information as listed in 2.2 shall be published promptly upon its creation, with the exception that if CRLs are used to provide Revocation information, they shall be published according to section 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 restrict access to those Participants with a specific need for the information.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

Each Subject must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the Certificate subjectName field of Certificates Issued under this Certificate Policy and in accordance with IETF PKIX RFC 5280 and its updates.

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.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The anonymity or pseudonymity of Subscribers is not permitted under this Certificate Policy.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

Fields that may be included are optional. Their interpretation for any entity shall be as follows:

Element	Description
Common Name	Common Name shall consist of the given name, middle name or middle initial (if the Subject has a middle name), and the family name of the Subject, in that order, separated by space characters.
Country name	The country where the entity resides or conducts business.
Organisation name	An organisation with which the entity has a significant relationship. The organisation name serves only as an additional identifier of the entity and does not imply employment or any authority to act on behalf of the organisation unless the Certificate and/or its policy specifically provide otherwise.
SubjectAlternative Name	Specified only in accordance with IETF PKIX RFC 5280. Where this specifies an email address, it is the electronic mail address at which the entity can receive electronic mail via the Internet.

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 POSSESSION OF PRIVATE KEY

The registration and/or issuance process shall involve a stage in which the applicant demonstrates possession of the Private Key. Technical means employed to ensure possession of Private Keys will be PKCS#10, other equivalent cryptographic mechanisms, or using a process specifically approved by the Policy Authority.

3.2.2 AUTHENTICATION OF ORGANISATION IDENTITY

Authentication of organisation identity is not supported as part of the PKI governed by this Certificate Policy.

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 PKI-DRS PKI Disclosure Statement. Additionally, the Issuing Authority may 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 Certificate applicants may include face-to-face authentication, but not require it. Individual identity may be authenticated by remote means.

Specific requirements for authentication of individual identity are provided in Section 2 of the PKI-DRS PKI Disclosure Statement. 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.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Non-verified subscriber information is not included in Certificates.

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) is not necessary as the only reason for obtaining an end entity certificate from the PKI-DRS is to sign digital deeds on behalf of an organisation.

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 of the PKI-DRS PKI Disclosure Statement**.**

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 not permitted.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Re-key of Certificates governed by this Certificate Policy is not permitted.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests at a minimum must include sufficient information to uniquely identify the Certificate to be Revoked and provide a valid reason for Revocation.

The risk for fraudulent misuse of the Private Key associated with the Certificate to be Revoked must be recognised. Where reliable authentication of the Revocation request isn't possible or even omitted, either the Issuing Authority or Registration Authority acting on its behalf, is authorised to conduct 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 Registration Authority.

Certificate applicants must comply with the procedures described in this document. Eligible Subscribers are specified in Section 15 of the PKI-DRS 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

The Issuing Authority or Registration Authority in its "Registration Policy and 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.
- Acceptance of the PKI-DRS Subscriber Agreement by the Subscriber.
- Compliance with this Certificate Policy and obligations of Subscribers as defined in Section 4 of the PKI-DRS PKI Disclosure Statement.

4.1.2.1 REGISTRATION AUTHORITIES AND THEIR REPRESENTATIVES

The Registration Authority and its representatives are authorised by the Issuing Authority. Issuance of Certificates to Registration Authority personnel shall be conducted by the Issuing Authority. See section 3.2.3

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.

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 approved, the Certificate application will be digitally signed for processing by the Certificate Manufacturer.

Where a Certificate application is rejected, the reasons for rejection may be given to the prospective applicant in accordance with the Issuing Authority or Registration Authority "Registration Policy and 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 Manufacturer (i.e. Certificate Authority) only in response to a properly constructed, signed and validated Certificate request from the relevant Registration Authority. Only an approved Registration Authority system 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 (or Certificate Authority) does not communicate with the Subscriber (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.

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

Use of a private-key for an activity or transaction approved under this Certificate Policy constitutes acceptance of the associated Certificate.

The Issuing Authority shall ensure that the Subscriber during application for or delivery of a Certificate, is provided with the details of terms and conditions stipulated in the governing Certificate Policy, associated Subscriber Agreement and any other applicable contractual commitments.

The Subscriber must acknowledge that it agrees to the terms and conditions stipulated in the Certificate policy and associated Subscriber Agreement and any other applicable contractual commitments prior to first use of the Certificate. 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.
- 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. This 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 PKI-DRS 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.

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 PKI-DRS PKI Disclosure Statement.

4.6 CERTIFICATE RENEWAL

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

Certificates may not be Renewed at any time during their Operational Period. Renewal of Expired or Revoked Certificates is not permitted. In these circumstances a new Certificate must be requested.

4.6.2 WHO MAY REQUEST RENEWAL

See Section 4.6.1

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

See Section 4.6.1.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See Section 4.6.1.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

See Section 4.6.1.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

See Section 4.6.1.

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 not permitted at any time during their Operational Period. Re-Key of Expired or Revoked Certificates is not permitted.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

See Section 4.7.1.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

See Section 4.7.1.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See Section 4.7.1.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

See Section 4.7.1.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

See Section 4.7.1.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See Section 4.7.1.

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.

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 services shall identify all Revoked Certificates; at least until their assigned validity period expires.

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

4.9.1 CIRCUMSTANCES FOR REVOCATION

The circumstances under which Certificate Revocation may be requested (and carried out) is 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 consider Revocation 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.
- When the Subscriber withdraws from or is no longer eligible to participate in the Public Key Infrastructure governed by this Certificate Policy.

The Issuing Authority or Registration Authority acting on its behalf may Revoke a Certificate when an Entity fails to comply with obligations set out in this Certificate Policy, any additional published documents defining practices to be followed by the entity, any other relevant agreement, or any applicable law.

4.9.2 WHO CAN REQUEST REVOCATION

The Revocation of a Certificate may be requested by any entity,

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

Approval of a Revocation request may only be granted by:

- 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.

A Revocation request may be generated by e-mail to the Issuing Authority or the 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 PKI-DRS 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 that permits authenticity and integrity of the Status Information to be verified. Revocation checking requirements shall be defined in the PKI-DRS Relying Party Agreement and in Section 5 of the PKI-DRS PKI Disclosure Statement.

Supported revocation status checking mechanisms must be defined in Section 17 of the PKI-DRS PKI Disclosure Statement.

4.9.7 CRL ISSUANCE FREQUENCY (IF APPLICABLE)

The frequency of CRL Issuance is defined in Section 17 of the PKI-DRS 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 PKI-DRS 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 PKI-DRS 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 Section 17 of the PKI-DRS PKI Disclosure Statement.

4.9.12 SPECIAL REQUIREMENTS RE KEY COMPROMISE

In the event of the compromise, or suspected compromise, of any Entity's Private Key, an Entity 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 PKI-DRS 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 PKI-DRS 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 PKI-DRS 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 on a case by case basis.

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.

Subscribers may not facilitate key escrow or recovery mechanisms locally.

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 this section of the Certificate Policy it indicates there are not specific prescribed requirements for the controls, configuration or security requirements.

Where not stipulated, specific details on controls operated for components of the PKI infrastructure 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 manufacture 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 Registration Authority gathers Registration or Revocation information, authenticates applicants, and forwards the results to the Certificate Manufacturer. The Registration Authority also initialises and loads Certificates and Private Keys into protected tokens.

In the case where the Registration Authority initialises and loads Certificates and Private Keys onto tokens, then the RA's physical security controls shall be as determined by the Policy Authority. Subscriber key material shall not be stored on RA workstations.

Where PINs, pass-phrases or passwords 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 PKI 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 Policy and 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 manufacturing operations.

All other duties associated with Certificate Manufacture or 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 Participant providing Trust Services.
- 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 Manufacturing 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 for PKI-DRS 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 the Certificate Policies 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.
- 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.

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 may also be required to retain additional information 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 upon request by any of the Participants involved in the transaction, or their 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.

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

Key changeover is not supported as part of the PKI governed by this Certificate Policy.

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 Public Key infrastructure processes from the effect of major compromises, failures or disasters. These shall enable the recovery of all Issuing Authority services.

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

In the case of comprise of a CA or CA-keys, the Issuing Authority shall as a minimum require the following:

- Immediately cause the suspension of the Certificate Status checking service for all Issued Certificates affected by a compromise, failure or disaster. This will stop any of these Certificates from being accepted by any Relying Party who follows proper Revocation checking procedures according to Section 5 of the PKI Disclose Statement
- Suspension of any further Certificate Issuance from the affected CA.

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. 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 Manufacture shall be designed to deal with any disruption to services and shall ensure managed, progressive recovery of components used to provide

the service. 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.

No specific business continuity requirements for the Registration Authority 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

Termination of a CA is regarded as the situation where all service associated with an Issuing Authority is terminated permanently. It is not the case where the service or elements of the service is transferred, such as between or to Certificate Manufacturers or responsibility for Certificates is transferred between Issuing Authorities, even if there is a change of CA-Keys.

Certificate Manufacturer – The specific circumstance related to termination of a CA must be prescribed by the Issuing Authority. At a minimum the following actions shall be taken under the direction of the Issuing Authority:

Inform both the Issuing Authority and Policy Authority for the governing Certificate Policy.

- Provide a notice period of 90 days.
- Revoke all relevant CA and Subscriber Certificates at the end of 90 days if required by the Issuing Authority.
- Arrange 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.

Registration Authority - At minimum the Registration Authority terminating service shall:

- Have all RA Certificates Revoked
- Ensure 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. Alternatively, with the approval of the Issuing Authority, records may be transferred to another Participant providing Trust Services, e.g. a new or alternative Registration Authority.

Registration Authority termination arrangements must be approved by the Issuing Authority or Auditors acting on its behalf.

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 PKI infrastructure 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 - Issuing Authority keys and CA-key pairs and signing keys shall be generated in a protected environment. CA-Key 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 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' Key Pairs shall be generated by the Registration Authorities approved by the Issuing Authority to conduct key generation. Procedures must be approved by the Issuing Authority or Auditors acting on its behalf.

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 6.2.1.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

The private key must be delivered to the Subscriber by the approved generator of the key and satisfying the requirements of 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.
- 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 Issuing Authority or Registration Authority "Registration Policy and 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 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 policy may be used in applications and services as listed in Section 2 of the PKI-DRS PKI Disclosure Statement. The only key usage that a Certificate may be used for is digital signature.

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

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 FIPS 140-2 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 keys that affects the outcome of Issued Certificates and Certificate Status Information services, at a minimum, two-person control is required.

6.2.3 PRIVATE KEY ESCROW

Subscribers shall not undertake escrow arrangements for their own Private Keys.

Participants providing trust services shall not provide Private Key escrow services.

6.2.4 PRIVATE KEY BACKUP

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

Subscribers shall not backup their own keys.

In all cases key backups shall at a minimum be protected to the standards commensurate with that stipulated for the primary version of the key.

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

6.2.5 PRIVATE KEY ARCHIVAL

No stipulation.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

Private Key transfer into or from a cryptographic module is not supported as part of the PKI governed by this Certificate Policy.

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 must be authenticated to their cryptographic module before the activation of the 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.

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 keys that affect the outcome of Issued Certificates and Certificate Status Information services, 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 two (2) years.

- Trust Service Provider trusted roles – two (2) 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.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

All Issuing Authority supporting CA-Keys and keys 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 keys or data to be protected. Where PINs, passwords or pass-phrases are used, an entity 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 keys 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 Keys 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:

- Access control to 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.
- Archival of Participant history and audit data.
- Audit of security related events.
- Trusted path for identification of PKI roles and associated identities.
- Recovery mechanisms for keys of PKI Participants providing trust services.

This functionality may be provided by the operating system, or through a combination of operating system, PKI CA software, 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 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

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.
- 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 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 not been assigned an OID.

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.

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 are not supported by the PKI governed by this Certificate Policy.

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 PKI-DRS PKI Disclosure Statement and may include internal auditing resources of Participants, subject to the approval of the Policy Authority.

For Certificate Manufacturers audit shall be conducted by an approved third-party 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 and any declared assurance or approval schemes under which Trust Services are operated.

Where the Participants providing Trust Services uses any designated authorised agents in order to provide service, 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 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 PKI 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.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE FEES

The Issuing Authority shall not charge Certificate Issuance fees.

9.1.2 CERTIFICATE ACCESS FEES

The Issuing Authority shall not charge fees for access to Certificate and Certificate Status Information.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

The Issuing Authority shall not charge fees for Certificate Revocation or Certificate status information access.

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 not permitted.

9.1.5 REFUND POLICY

Refunds are specified in the commercial arrangements between the Issuing Authority and Subscribers.

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

Arrangements to fulfil liability commitments are specified in Section 6 of the PKI-DRS PKI Disclosure Statement.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

The Issuing Authority does not provide 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 and secret keys and associated activation data used or otherwise handled by Participants operating under this Certificate Policy shall be kept confidential unless required otherwise by law.

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 will only be disclosed by the Certificate Manufacturer in accordance with the governing Certificate Policy or as required by law.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

Certificates and Certificate Status Information are not classified as Confidential or as private. Identification information or other personal or 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. Responsibly to maintain the confidentiality of information is devolved to all Participants via this Certificate Policy 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 Data Protection Act 2018, and any other relevant 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 have agreed 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 particular purposes. They have also agreed 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 PKI-DRS 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. Responsibly to protect privacy information is devolved to all Participants via this Certificate Policy 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 so required by due process of law and subject to any duty of confidence to provide such information and/or data as is demanded 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 Management Authority. In the case of confidential or privacy information approval of the data subject shall 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 licence to make use of the materials only for the purposes and in compliance with the terms of the governing Certificate Policy, relevant Certification Practice Statements and any applicable contract, and in particular 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 the governing Certificate Policy shall ensure that all information supplied to other parties operating under the governing Certificate Policy does not infringe upon any third-party rights including intellectual property rights.

All parties operating under the governing Certificate Policy shall ensure that in using the 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

No representations or warranties are made by the Issuing Authority in respect of this Certificate Policy.

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.

9.8 LIMITATIONS OF LIABILITY

By signing a Certificate, the 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 Public/Private Key pairs Issued under this Certificate Policy for any use other than in accordance with this Certificate Policy and any other agreements.

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, delict, 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 in the case of the Issuing Authority's negligence, willful misconduct, or where otherwise required by applicable law.

Nothing in this Certificate Policy excludes or restricts 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, delict (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 delict, contract or any other reason with respect to any service associated with the Issuance, use of, or reliance upon Certificates or associated Public/Private key pairs Issued under this policy, in excess of that specified in Section 6 of the PKI-DRS 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 Public/Private Key pairs Issued under this policy in a manner that is not in accordance with this policy; and
- Subscribers' negligence, default or breach of this 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 agreement with immediate effect if the Subscriber(s) commits a material breach of any of the terms of this Policy and (if such a breach is remediable) fails to remedy that breach within 30 days of being notified in writing of the breach.

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 clause 9.10.3 shall survive termination.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 SUBSCRIBERS

Whenever any Subscriber 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 e-mail or by paper-based communications. Electronic communications shall be effective upon the sender receiving a valid acknowledgment of receipt from the 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, return receipt requested, addressed to the Issuing Authority as

detailed in Section 1 of the PKI-DRS PKI Disclosure Statement under Issuing Authority. All such communications shall be effective upon receipt.

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

- Changes in name or e-mail address.
- 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 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 in 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 are awaiting comments.
- Changes which, in the judgement of the Policy Authority, will not materially impact a substantial majority of the Subscribers or Relying Parties using this Certificate Policy.
- Changes which, in the judgement of the Policy Management Authority, are likely to have a material impact upon a significant number of users of this Certificate Policy.

Where the amendments are likely to have a major impact on the majority of users of this Certificate Policy 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 users of this Certificate Policy Certificate Policy 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 who shall ensure that notice of such proposed changes is posted in their Repositories 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 users of this Certificate Policy 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 users of this Certificate Policy 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

This Certificate Policy has not been assigned an OID.

9.13 DISPUTE RESOLUTION PROVISIONS

All disputes shall be referred in writing to the Issuing Authority. The Issuing Authority shall deal with such disputes in accordance with its dispute resolution process specified in section 10 of the PKI-DRS PKI Disclosure Statement.

9.14 GOVERNING LAW

This Certificate Policy shall be governed by the law of Scotland and the parties submit to the exclusive jurisdiction of the courts of Scotland. 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 by mediation between the parties according to Section 9.13.

9.15 COMPLIANCE WITH APPLICABLE LAW

All Participants within the PKI 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 parties acknowledge that, except for documents expressly referred to or incorporated by reference herein, this Policy constitutes the entire agreement and understanding of the parties and supersedes any previous agreement between the parties relating to the subject matter of this Policy. For the purposes of this clause, such documents shall be:

- PKI-DRS PKI Disclosure Statement
- PKI-DRS Relying Party Agreement
- PKI-DRS Subscriber Agreement
- PKI-DRS Glossary of Terms

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

9.16.2 ASSIGNMENT

This Certificate Policy shall be binding upon and inure to the benefit of all parties hereto. The rights and obligations detailed in this Certificate Policy are not assignable by the parties 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 party in enforcing against any other party 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 party under this Certificate Policy. No right, power or remedy in this Certificate Policy conferred upon or reserved for a party is exclusive of any other right, power or remedy available to

that party. Each party 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 Policy if it is prevented from or delayed in performing its obligations under this Policy, or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control, including, without limitation, strikes, lock-outs or other industrial disputes (whether involving the workforce of the Issuing Authority or any other party), failure of a utility service or transport network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors.

If any such events affecting the availability of or access by a Relying Party to Certificate Status Information as described in the preceding paragraph continue for a continuous period of more than 72 hours, the Issuing Authority may terminate this Policy by written notice to the other parties.

9.17 OTHER PROVISIONS

9.17.1 CERTIFICATE POLICY CONTENT

Section and paragraph headings shall not affect the interpretation of this 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 Policy shall be enforceable under the Contracts (Rights of Third Parties) Act 1999 by a third party. The parties who have such rights are the Participants.

GLOSSARY

Terms used in this Certificate Policy are defined in the PKI-DRS Glossary of Terms at https://www.ros.gov.uk/services/digital-discharge-service/dds-for-lenders-t-and-c.