ENTRUST (EUROPE) LTD MASTER CERTIFICATION PRACTICE STATEMENT

A Certification Practice Statement applying to digital certificates as manufactured by Entrust (Europe) Ltd

Version v1.9 (RFC 3647)

CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

A Certification Practice Statement (CPS) is a set of statements that indicate the means by which the Certificate Manufacturer will manufacture certificates for a particular community and / or class of application so as to satisfy the requirements specified in the governing Certificate Policy ("CP").

This Practice Statement applies to:

- Services and facilities provided by Entrust (Europe) Ltd as part of its Certificate Factory and certification services that include, but are not limited to, Issuing, Managing, Revoking, and Renewing Certificates.
- All parties authorised to participate in Public Key Infrastructures (PKIs) whereby compliance with this Certification Practice Statement is prescribed via a Certificate Policy, agreement or contractual requirement. This includes, but is not limited to, all Participants whose organisations provide subordinate Certificate Authorities, Registration Authorities, Repositories or validation services.
- All requirements for the issuance and management of Certificates conducted under the control of this Certification Practice Statement

Specific terms are used throughout this document to define parties, processes, technology elements and applicable legal and regulatory requirements. These terms are explained in Section 1.3 and the Entrust (Europe) Ltd document “Glossary of Terms”.

This Certification Practice Statement is structured according to the guidelines provided by IETF RFC 3647 with extensions defined where appropriate to meet the requirements of English Law & prevailing regulatory requirements.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is entitled the “Entrust (Europe) Ltd Certification Practice Statement”. It is defined as “A Certification Practice Statement applying to digital certificates as manufactured by Entrust (Europe) Ltd”

This Certification Practice Statement document is registered with Entrust (Europe) Ltd operating in an authorised administrative role for the relevant Issuing Authority.

1.3 PKI PARTICIPANTS

This CPS defines how the Certificate Manufacturer, Issuing Authority[i] and all other approved Participants must satisfy the requirements of the governing Certificate Policy.

1.3.1 CERTIFICATION AUTHORITIES

RFC 3647 defines Certification Authorities as the entities that issue Certificates. Within the scope of this CPS Certification Authority is synonymous with Issuing Authority.

1.3.1.1 THE ISSUING AUTHORITY

The Issuing Authority is the entity listed in the issuer field of a Digital Certificate. The Issuing Authority has the ultimate responsibility for deciding who may be issued with a digital certificate carrying its name and is the only entity with which End-Entities have any form of direct or indirect contractual relationship. The Issuing Authority is by definition the entity or organisation who is named in the "Issuer" field of a Certificate.

1.3.1.2 CERTIFICATE MANUFACTURER

The Certificate Manufacturer, which provides certificate management operational services for the Issuing Authority as specified in the governing Certificate Policy. The Certificate Manufacturer is approved by the Issuing Authority to manage certificates on behalf of other entities participating in the public key infrastructure governed by the governing Certificate Policy. This CPS document defines how the Certificate Manufacturer supports the governing Certificate Policy.

1.3.2 REGISTRATION AUTHORITIES

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

1.3.3 SUBSCRIBERS

A Subscriber is an entity (such as a person or organisation) that has been authorised directly, or indirectly, by an organisation to receive and use a Certificate. They interact with the Registration Authorities under the overall control of the Issuing Authority. 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.

1.3.4 SUBJECTS

Where a Certificate is issued to a device or Certificate holder, who does not directly contract with the Issuing Authority, the Subscriber or an entity acting on behalf of the Subscriber will accept the terms and conditions on behalf of the Subject that is identified in the Certificate. The Subject must be under the jurisdiction and control of the Subscriber and comply with all relevant aspects of this Certificate Policy and other agreements and obligations undertaken by the Subscriber. In all cases the Subscriber is

responsible for compliance with the Certificate Policy and all other obligations applicable to it and the Subject.

1.3.5 RELYING PARTIES

A Relying Party is an entity that does not necessarily hold a Certificate, but even so, during the course of a transaction, may be a recipient of a certificate and who therefore relies on that Certificate and / or Digital Signatures created using that Certificate**.**

1.3.6 OTHER PARTICIPANTS

1.3.6.1 POLICY AUTHORITY

The Policy Authority has ultimate responsibility for governance and control, of the issuance, management and usage of Digital Certificates issued under the governing the Certificate Policy. Simply stated, the Policy Authority is the entity that sets the rules under which the PKI is to be operated.

1.3.6.2 REPOSITORY

A Repository is the Participant organisation that holds data in support of PKI Operations. This includes policy and related documentation, Certificates and Certificate Status information.

1.4 CERTIFICATE USAGE

Certificate usage is ultimately defined by the Certificate Profile which is formally approved by the Policy Authority and the Issuing Authority.

1.4.1 APPROPRIATE CERTIFICATE USES

The categories of transactions, applications, or purposes for which certificates are issued under this CPS are set forth in the governing Certificate Policy**.**

1.4.2 PROHIBITED CERTIFICATE USES

The categories of transactions, applications, or purposes for which certificates are issued under this CPS are set forth in the governing Certificate Policy**.**

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

The Policy Authority is responsible for approving rights, obligations, liabilities and all other terms and conditions contained in the governing Certificate Policy.

Entrust (Europe) Ltd is responsible for this CPS, its management and change control.

Entrust (Europe) Ltd can be contacted as follows:

Entrust (Europe) Ltd,

Building 273,

New Greenham Park,

THATCHAM ,

RG19 6HN,

United Kingdom.

Tel: +44 (0)1635 231361

Fax: +44 (0) 1635 231366

Email: info@trustis.com

1.5.2 CONTACT PERSON

In the first instance the Issuing Authority should be contacted regarding the contents of this CPS.

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

In the first instance the Issuing Authority should be contacted regarding the suitability of this CPS to support the governing Certificate Policy.

1.5.4 CPS APPROVAL PROCEDURES

The requirements for approval of this CPS in the context of operation in accordance with a specific Certificate Policy are defined in the governing Certificate Policy.

Entrust (Europe) Ltd manages and approves the content of this CPS.

1.6 DEFINITIONS AND ACRONYMS

A definition of the terms used in this CPS may be found in the Entrust (Europe) Ltd document “Glossary of Terms”.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

A repository may be either electronic or physical. Details of the Repository are set forth in the governing Certificate Policy. On behalf of the Issuing Authority the Certificate Manufacturer makes Certificate Status Information available to the Repository in accordance with the governing Certificate Policy.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The Repository publishes on behalf of the Issuing Authority:

- Any governing Certificate Policy(s)
- Other contractual and policy information relevant to the operations controlled by this CPS whether undertaken by the Issuing Authority or any other Participant acting as on its behalf.
- The information that will allow the authenticity of the Certificate of the Issuing Authority to be verified
- Certificate Status Information (where specified in the governing Certificate Policy)
- Certificate information (where specified in the governing Certificate Policy)
- All CA-Certificates of Certificate Authorities operating under the control of the Issuing Authority.

The Repository excises control over the information to restrict access to those who are authorised participants in the Public Key Infrastructure. The repository publishes this CPS; however, access is restricted to Participants that have specific need for the information contained herein.

The location for electronic access to information is published in the governing Certificate Policy and in the Certificates issued in accordance with this CPS.

Paper copies of documentation will be made available on request (a charge may be made). Application should be made to the Issuing Authority.

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificates are published once they are manufactured. Certificate Status Information is published in accordance with the governing Certificate Policy. Other materials such as documents (for example Certificate Policies) are republished as required by the change control process for the document.

2.4 ACCESS CONTROLS ON REPOSITORIES

Access to the Repository is (at a minimum) made available to those participating in the PKI. Controls to prevent unauthorised access or modification are in place. These controls are applied selectively as appropriate to the particular type of information.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

Naming conventions are complied with and enforced via a formal process which requires approval by the Issuing Authority for naming used in all Certificates.

3.1.1 TYPES OF NAMES

Naming conventions are operated in conformance with the governing Certificate Policy.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

Naming conventions are operated in conformance with the governing Certificate Policy.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The Issuing Authority is responsible for deciding whether or not Subscribers can be anonymous or pseudonymous, and if they can, what names are assigned to or can be used by anonymous Subscribers.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

Name forms will be interpreted in conformance with the governing Certificate Policy.

3.1.5 UNIQUENESS OF NAMES

Name uniqueness will be interpreted in conformance with the governing Certificate Policy.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

Neither the Policy Authority (including the associated Certificate Manufacturer) nor the Issuing Authority are liable for the inclusion of trademarks, trade names or other information under restricted use. Subscribers are required to declare legitimacy of their registration details to the Issuing Authority as part of the Registration Process.

Name claim disputes are resolved in conformance with the governing Certificate Policy.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

Registration approval by an authorised Registration Authority, acting under the authority of an Issuing Authority, is required prior to Certificate issuance. Technical means employed to ensure possession of Private Keys, will be PKCS#10, other equivalent cryptographic mechanism or using a process specifically approved by the Certificate Manufacturer.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

Organisation Identity authentication by the Registration Authorities is carried out as defined in the governing Certificate Policy. The Issuing Authority defines through its enrolment requirements or equivalent documents the standards of authentication required. The Issuing Authority, through its "Registration Authority Procedures" enforces that authentication is robustly completed to the required standards.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

Entity authentication by the Registration Authorities is carried out as defined in the governing Certificate Policy. The Issuing Authority defines through its enrolment requirements or equivalent documents the standards of authentication required. The Issuing Authority, through its "Registration Authority Procedures" enforces that authentication is robustly completed to the required standards.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

The collection and use of non-verified Subscriber information is defined by, and the responsibility of, the Issuing Authority. The collection and use of non-verified Subscriber information by the Registration Authorities is carried out in accordance with the governing Certificate Policy as described in the Issuing Authority "Registration Policy and Procedures".

The collection and retention of all information provided by Subscribers is conducted in accordance with the Data Protection Act and the Certificate Manufacturer and Registration Authority Procedures.

3.2.5 VALIDATION OF AUTHORITY

Validation of authority (i.e. the determination of whether a Subscriber has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a certificate) is the responsibility of the Registration Authorities and is carried out as described in the Issuing Authority "Registration Authority Procedures".

3.2.6 CRITERIA FOR INTEROPERATION

The criteria which another Certification Authority wishing to operate within, or interoperate with, the PKI covered by this CPS must satisfy will be defined by the Policy Authority for the relevant CA. The Policy Authority will also determine whether or not the CA concerned is suitable for such operations or interoperation.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Routine Re-Key requests to the Registration Authorities, including the identification and authentication of the requester, are carried out as described in the Issuing Authority "Registration Policy and Procedures". All Re-Key requests require at a minimum confirmation of the identity of the requestor.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Re-Key after revocation requests to the Registration Authorities, must at a minimum include the identification and authentication of the requester to at least the authentication standards defined in the governing Certificate Policy. This by definition is an Issuance of a new certificate. Re-Key and Issuance procedures are described in the Issuing Authority "Registration Authority Procedures".

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests received by the Registration Authorities must, at a minimum, be subject to the identification and authentication of the requester and information which uniquely identifies the certificate to be revoked. Such checks and the Revocation are carried out as described in the Issuing Authority "Registration Authority Procedures".

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

The decision on who can submit a Certificate application is made by the Issuing Authority; and defined in the governing Certificate Policy. This decision is implemented by the Registration Authority and carried out as described in the Issuing Authority "Registration Authority Procedures".

4.1.2 ENROLMENT PROCESS AND RESPONSIBILITIES

The enrolment process, and the responsibilities of the various parties, is defined by the Issuing Authority in the governing Certificate Policy and implemented by the Registration Authority. The enrolment process is described in the Issuing Authority "Registration Authority Procedures".

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The Issuing Authority is responsible for the definition of the process to be followed in order to identify and authenticate the applicant. The processing of applications and implementation of procedures may

be conducted by one or more Registration Authorities and / or Local Registration Authorities. The Registration Authority is responsible for the implementation of this process which is described in the Issuing Authority "Registration Authority Procedures".

Checks of CAA records are only conducted for services where the Certificate Policy (Section 2 of PDS) indicates this requirement. In the case of such services, the procedure for CAA checks is described in the Issuing Authority "Registration Authority Procedures".

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

The Issuing Authority is responsible for the definition of the process to be followed to decide whether to approve or reject a certificate application. The Registration Authority is responsible for the implementation of this process which is described in the Issuing Authority "Registration Authority Procedures".

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

The time to process a certificate application is made up of two elements:

- The time for the certificate application to be approved and actioned by the Registration Authority. The maximum time for this element will be defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".
- The time taken for the Certificate Manufacturer to respond to the authorised certificate application and generate the required Certificate. Any maximum time for this element may be defined in the contract between the Issuing Authority and the Certificate Manufacturer.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

Certificates are automatically issued by the Certificate Manufacturer (or Certificate Authority) in response to a properly constructed and signed request from the relevant Registration Authority. Only an approved Registration Authority system can communicate with the associated Certificate Authority to submit a certificate request. The Certificate issuance process is described in the Issuing Authority "Registration Authority Procedures".

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

The Certificate Manufacturer (or Certificate Authority) does not communicate directly with the Subscriber regarding certificate issuance. Rather the Registration Authority is responsible for such notification as described in the Issuing Authority "Registration Authority Procedures". Notification is provided by either manual or automatic means.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

The definition of the conduct that constitutes Certificate acceptance is set out by the Issuing Authority and published as appropriate. In general Certificate applicants are provided formal notification of the Certificate Policy, Subscriber Agreement and any additional specific terms applicable to Subjects. They are directed to only install and / or use a Certificate provided that they accept, and comply with, the governing Certificate Policy and relevant associated documentation.

Subscribers, where they are not Subjects, must formally agree to, and comply with, the governing Certificate Policy and Subscriber Agreement. Subscribers are notified of, and are required to fulfil, their obligations relating to Subjects to whom Certificates has been issued under their agreement with the Issuing Authority.

Installation and or use of the Certificate are deemed as acceptance of the Certificate and the governing Certificate Policy.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

The Certificate Manufacturer (or Certificate Authority) places the issued Certificate in the location specified by the Issuing Authority. It is the responsibility of the Issuing Authority to decide what further "publication" of the Certificate should be undertaken.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

The Certificate Manufacturer (or Certificate Authority) does not inform any entities other than Participants of the issuance of a Certificate. It is the responsibility of the Issuing Authority to decide what notification of Certificate issuance should take place.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

The definition of the use of the Subscriber's Private Key and Certificate is set out by the Issuing Authority and published as appropriate. The Certificate Manufacturer (or Certificate Authority) does not have any responsibility in this area.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

The definition of the Relying Party responsibilities relating to the use of a Subscriber's Public Key and Certificate is set out by the Issuing Authority and published as appropriate. The Certificate Manufacturer (or Certificate Authority) does not have any responsibility in this area.

4.6 CERTIFICATE RENEWAL

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

The circumstances under which Certificate Renewal may be 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 (for example that a Certificate Renewal is not permitted) as defined in the governing Certificate Policy and described in the Issuing Authority "Registration Authority Procedures".

4.6.2 WHO MAY REQUEST RENEWAL

The decision on who may submit a Certificate renewal request is made by the Issuing Authority; this decision is implemented by the Registration Authority and carried out as described in the Issuing Authority "Registration Authority Procedures".

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

Certificate renewal requests will be received by the Registration Authority who will process them in accordance with the instructions defined by the Issuing Authority in the governing Certificate Policy and as described in the Issuing Authority "Registration Authority Procedures".

Certificate renewals are automatically processed by the Certificate Manufacturer (or Certificate Authority) in response to a properly constructed and signed certificate request from the relevant Registration Authority. Request procedures must at a minimum always include authentication of the Subject (Subscriber) of the existing Certificate. This is normally via presentation of an existing valid Certificate.

Extension of Certificate validity beyond the initial validity period for a Key Pair, as defined in Expiry Date field of the Issued Certificate is not supported.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

The Certificate Manufacturer (or Certificate Authority) does not inform any entities other than Participants of the renewal of a Certificate. It is the responsibility of the Issuing Authority to decide what notification of certificate renewal should take place.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

The definition of the conduct that constitutes certificate acceptance is set out by the Issuing Authority and published as appropriate. In general Certificate applicants are provided formal notification of the Certificate Policy, Subscriber agreement and any additional specific terms applicable to Subjects. They

are directed to only install and or use a Certificate provided that they accept, and comply with, the governing Certificate Policy and relevant associated documentation.

Subscribers, where they are not Subjects, must formally agree to, and comply with, the governing Certificate Policy and Subscriber Agreement. Subscribers are notified of, and are required to fulfil, their obligations relating to Subjects to whom Certificates has been issued under their agreement with the Issuing Authority.

Installation and / or use of the Certificate are deemed as acceptance of the Certificate and the governing Certificate Policy.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

The Certificate Manufacturer (or Certificate Authority) places the renewed certificate in the location specified by the Issuing Authority. It is the responsibility of the Issuing Authority to decide what further "publication" of the certificate should be undertaken.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

The Certificate Manufacturer (or Certificate Authority) does not inform any entities other than Participants of the renewal of a certificate. It is the responsibility of the Issuing Authority to decide what notification of Certificate issuance should take place.

4.7 CERTIFICATE RE-KEY

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

The circumstances under which certificate Re-Key may be carried out is defined by the Issuing Authority and defined in the governing Certificate Policy. The Registration Authority is responsible for the implementation of the decision of the Issuing Authority as described in the Issuing Authority "Registration Authority Procedures".

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

The decision on who can submit a request for certification of a new Public Key (Re-Key) is made by the Issuing Authority and defined in the governing Certificate Policy, this decision is implemented by the Registration Authority and carried out as described in the Issuing Authority "Registration Authority Procedures".

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

Certificate Re-Key requests will be received by the Registration Authority who will process them in accordance with the instructions defined by the Issuing Authority as described in the Issuing Authority "Registration Authority Procedures".

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

Request procedures must at a minimum include authentication of the Subject (Subscriber) of the existing Certificate. This is normally via presentation of an existing valid Certificate.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

The Certificate Manufacturer (or Certificate Authority) does not inform any entities other than Participants of the issue of a Certificate. It is the responsibility of the Issuing Authority to decide what notification of Certificate Re-Key should take place.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

The definition of the conduct that constitutes certificate acceptance is set out by the Issuing Authority and published as appropriate. In general certificate applicants are directed to only install the certificate provided that they accept, and agree to comply with, the terms and conditions outlined in the governing Certificate Policy. In general Certificate applicants are provided formal notification of the Certificate Policy, Subscriber Agreement and any additional specific terms applicable to Subjects. They are directed to only install and / or use a Certificate provided that they accept, and comply with, the governing Certificate Policy and relevant associated documentation.

Subscribers, where they are not Subjects, must formally agree to, and comply with, the governing Certificate Policy and Subscriber Agreement. Subscribers are notified of, and are required to fulfil, their obligations relating to Subjects to whom Certificates has been issued under their agreement with the Issuing Authority.

Installation and / or use of a Certificate are deemed as acceptance of the Certificate and the governing Certificate Policy.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

The Certificate Manufacturer (or Certificate Authority) places the Re-Keyed Certificate in the location specified by the Issuing Authority. It is the responsibility of the Issuing Authority to decide what further "publication" of the Certificate should be undertaken.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

The Certificate Manufacturer (or Certificate Authority) does not inform any entities other than Participants of the Re-Key of a Certificate. It is the responsibility of the Issuing Authority to decide what notification of Certificate issuance should take place.

4.8 CERTIFICATE MODIFICATION

4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

Certificate Modification is not permitted under this CPS. Change to the Subject name of a Certificate, or any substantive component of a Certificate, will be subject to re-Issuance or Renewal criteria as defined in the relevant section of the governing Certificate Policy.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

See Section 4.8.1

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

See Section 4.8.1

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See Section 4.8.1

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

See Section 4.8.1

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

See Section 4.8.1

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See Section 4.8.1

4.9 CERTIFICATE REVOCATION AND SUSPENSION

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 in the governing Certificate Policy. The Registration Authority is

responsible for the implementation of the decision of the Issuing Authority as described in the Issuing Authority "Registration Authority Procedures".

In the Interests of preserving security and integrity, the Certificate Manufacturer or any Participant may request the revocation of a certificate.

4.9.2 WHO CAN REQUEST REVOCATION

The decision on who can submit a certificate revocation request is made by the Issuing Authority and published in the governing Certificate Policy; this decision is implemented by the Registration Authority and carried out as described in the Issuing Authority "Registration Authority Procedures".

4.9.3 PROCEDURE FOR REVOCATION REQUEST

Certificate Revocation requests will be received by the Registration Authority or directly by the Issuing Authority. They shall be processed them in accordance with the instructions defined by the Issuing Authority as described in the Issuing Authority "Registration Authority Procedures".

At a minimum, the procedure for processing revocation requests shall include authentication of the requestor see Section 3.4

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

4.9.4 REVOCATION REQUEST GRACE PERIOD

The grace period which will apply to Certificate Revocation requests is defined by the Issuing Authority in the governing Certificate Policy and implemented as described in the Issuing Authority "Registration Authority Procedures".

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

This time to process a certificate revocation request is made up of two elements:

- The time for the certificate revocation request to be approved and actioned by the Registration Authority (including any grace period – see Section 4.9.4). The maximum time for this element will be defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".
- The time taken for the Certificate Manufacturer to respond to the authorised Certificate Revocation request. The time for this element that the Certificate Manufacturer will comply with is defined in the governing Certificate Policy or contract between the Issuing Authority and the Certificate Manufacturer.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

The mechanisms, if any, that a Relying Party may use (or where appropriate must use) in order to check the status of Certificates on which they wish to rely is be defined by the Issuing Authority in the governing Certificate Policy and described in the Issuing Authority document "Relying Party Agreement"

4.9.7 CRL ISSUANCE FREQUENCY (IF APPLICABLE)

The minimum frequency of CRLs issued by the Certificate Manufacturer will be agreed between the Issuing Authority and the Certificate Manufacturer and published by the Issuing Authority in the governing Certificate Policy.

CRLs may be issued more frequently than defined in the governing Certificate Policy but shall have at a maximum a lifetime (as defined by Effective Date and Next Update) no greater than the frequency interval defined in the governing Certificate Policy. This provides Relying Parties (should they wish to exploit it) more detailed information relating to Certificate Status without excessive CRL lookup activity, or damage to the resilience of their application.

4.9.8 MAXIMUM LATENCY FOR CRLS (IF APPLICABLE)

The maximum latency of CRL issuance will, if applicable, be agreed between the Issuing Authority and the Certificate Manufacturer and published by the Issuing Authority in the governing Certificate Policy.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

The availability of on-line revocation / status checking will be agreed between the Issuing Authority and the Certificate Manufacturer and defined by the Issuing Authority in the governing Certificate Policy.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

The requirements on Relying Parties to perform on-line revocation / status checks will be defined by the Issuing Authority in the governing Certificate Policy and the Relying Party Agreement.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

The availability of other forms of revocation advertisement will be agreed between the Issuing Authority and the Certificate Manufacturer and defined by the Issuing Authority in the governing Certificate Policy.

4.9.12 SPECIAL REQUIREMENTS RE KEY COMPROMISE

Any variations of the above stipulations for which Suspension or Revocation is the result of Private Key compromise (as opposed to other reasons for Suspension or Revocation) will be defined and published by the Issuing Authority.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

The circumstances under which Certificate Suspension may be requested is defined by the Issuing Authority and published in the governing Certificate Policy. The Registration Authority is responsible for the implementation of the decision of the Issuing Authority as described in the Issuing Authority "Registration Authority Procedures".

4.9.14 WHO CAN REQUEST SUSPENSION

Who can submit a Certificate Suspension request is prescribed by the Issuing Authority and published in the governing Certificate Policy; this decision is implemented by the Registration Authority and carried in accordance with the Issuing Authority "Registration Authority Procedures".

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

Certificate Suspension requests will be received by the Registration Authority who will process them in accordance with the instructions defined by the Issuing Authority as described in the Issuing Authority "Registration Authority Procedures".

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

4.9.16 LIMITS ON SUSPENSION PERIOD

The decision on the duration of a Certificate Suspension is made by the Issuing Authority; this decision is implemented by the Registration Authority and carried out as described in the Issuing Authority "Registration Authority Procedures".

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

The operational characteristics of any Certificate Status checking services that are available to the Relying Parties are defined and published by the Issuing Authority in the governing Certificate Policy.

4.10.2 SERVICE AVAILABILITY

The availability of a Certificate Status checking services is defined by the Issuing Authority and published in the governing Certificate Policy.

4.10.3 OPTIONAL FEATURES

The optional features of any certificate status checking services that are available to the Relying Parties will be defined and published by the Issuing Authority.

4.11 END OF SUBSCRIPTION

For Subscribers the actions to be taken at the end of the subscription are defined by the Issuing Authority and published in the governing Certificate Policy.

In the event of the termination by a customer of a full PKI service the actions to be taken will be, where possible, agreed between the Issuing Authority and the Certificate Manufacturer. Where a full infrastructure is terminated completely the destruction of Keys and the removal of components is described in the Certificate Manufacturer Procedures.

4.12 KEY ESCROW AND RECOVERY

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

The use of Key escrow services and the associated recovery policies are defined by the Issuing Authority and published in the governing Certificate Policy.

Key escrow of End-Entity Subscriber Private Keys is not provided as part of the Certificate Manufacturer services.

Recovery mechanism for CA-Keys is based on n from m Key splitting. The specific arrangements for CA-Key management are agreed between the Issuing Authority and Certificate Manufacturer. In all cases multi person control is required for CA-Key recovery.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

Session Key encapsulation, and the associated recovery policies and procedures, are defined by the Issuing Authority and published in the governing Certificate Policy.

Session Key encapsulation is not provided as part of the Certificate Manufacturer services.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 SITE LOCATION AND CONSTRUCTION

The Trust Service Centre (TSC) and the backup facility, the Alternative Trust Service Centre (ATSC), are geographically separated and dependent upon separate supplies for services.

The Certificate Manufacturer operates its Trust Service Centre under a strategy of strength in depth. Physical security controls are implemented to control access to all operational and support resources as well as for operational Trust Services. These controls include the PKI systems, PKI workstation remote

management facilities and all cryptographic hardware modules. All reserve, backup and emergency recovery facilities are maintained under the same level of physical security protection.

The CA-Keys used for signing Certificates and Certificate Status Information are stored in Hardware Security Modules such that they cannot be removed from the device intact. The Hardware Security Modules are certified to FIPS140-1 level 3.

The Certificate Manufacturing facility is described in the "Certificate Manufacturer Physical Description".

Registration Authority systems are located as described in the Issuing Authority "Registration Authority Physical Description".

5.1.2 PHYSICAL ACCESS

Physical access to systems used for Certificate Manufacture is restricted to authorised persons who are members of the operations staff. Essential technical support personnel are admitted only when approved and accompanied by an authorised person. These controls are described in the "Certificate Manufacturer Procedures".

Physical access to the Registration Authority systems is described in the Issuing Authority "Registration Authority Procedures".

5.1.3 POWER AND AIR CONDITIONING

The Certificate Manufacturing facility has power and air conditioning facilities including backup power these are described in the "Certificate Manufacturer Physical Description"

Registration Authority systems operate with the power and air conditioning of the facility in which they are installed as described in the Issuing Authority "Registration Authority Physical Description".

5.1.4 WATER EXPOSURES

The Certificate Manufacturing facility has protection against water exposure as described in the "Certificate Manufacturer Physical Description"

Registration Authority systems have the level of protection provided by the facility in which they are installed as described in the Issuing Authority "Registration Authority Physical Description".

5.1.5 FIRE PREVENTION AND PROTECTION

The Certificate Manufacturing facility has fire protection and detection facilities as described in the "Certificate Manufacturer Physical Description"

Registration Authority systems have the level of fire protection provided by the facility in which they are installed as described in the Issuing Authority "Registration Authority Physical Description".

5.1.6 MEDIA STORAGE

All media related to the Certificate Manufacture activity is stored within the Certificate Manufacturing facility as described in the "Certificate Manufacturer Physical Description". Access to this media is controlled as described in the "Certificate Manufacturer Procedures".

All media related to the Registration Authority activities is stored as described in the Issuing Authority "Registration Authority Physical Description". Access to media related to the Registration Authority activities is described in the Issuing Authority "Registration Authority Procedures".

5.1.7 WASTE DISPOSAL

All sensitive waste material is disposed of as described in the "Certificate Manufacturer Procedures".

All material related to the Registration Authority activities is disposed of as described in the Issuing Authority "Registration Authority Procedures".

5.1.8 OFF-SITE BACKUP

All material which is moved off-site from the Certificate Manufacturer facility is protected both while in transit and while stored at the off-site location as described in the "Certificate Manufacturer Procedures".

The protection of all material related to the Registration Authority which is to be stored off-site is described in the Issuing Authority "Registration Authority Procedures".

5.2 PROCEDURAL CONTROLS

All procedural controls are designed to ensure compliance with all governing Certificate Policies supported by the Certificate Manufacturer and using this CPS.

5.2.1 TRUSTED ROLES

All activities that may impact PKI facilities, support services, authentication or validity of Certificates require pre-vetted, authorised and approved staff. Such staff are allocated trusted roles to ensure conformance with governing Certificate Policy.

The definitions of the specific roles associated with the secure operation of the Certificate Manufacturer Facility, and the lists of named personnel authorised to perform these roles, are described in the "Certificate Manufacturer Procedures".

The definition of those authorised to operate the Registration Authority, including the associated systems and processes, and the allocation of specific trusted roles, are described in the Issuing Authority "Registration Authority Procedures".

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Critical functions within the Certificate Manufacturer are performed under multi-person control, these tasks and the associated authorised persons are described in the "Certificate Manufacturer Procedures". Both procedural and physical mechanisms are used to enforce multi person control.

Operational CA-Keys are always managed under multi person control.

Where applicable multi-person controls relating to the Registration Authority, including the associated systems is described in the Issuing Authority "Registration Authority Procedures".

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

Identification and authentication of staff for the various roles is in conformance with the governing Certificate Policy.

All persons who perform a trusted role within the Certificate Manufacturer have both their identity and their current authority to perform that role verified as described in the "Certificate Manufacturer Procedures".

The procedure for the verification of the identity of staff authorised to operate the Registration Authority, including the associated systems and processes, is described in the Issuing Authority "Registration Authority Procedures".

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

Those roles and duties within the Certificate Manufacturer that cannot be performed by single individuals are described in the "Certificate Manufacturer Procedures". This document also identifies the assignment of personnel to roles as well as the duties and responsibly associated with specific roles.

Similar controls for Registration Authorities are described in the Issuing Authority "Registration Authority Procedures".

5.3 PERSONNEL CONTROLS

All personnel controls are designed to ensure compliance with all governing Certificate Policies supported by the Certificate Manufacturer and using this CPS.

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

Background, qualifications, experience security clearance and other personnel criteria are prescribed and checked via formal mechanisms to ensure support for governing Certificate Policy.

All members of staff employed by the Certificate Manufacturer (and where applicable staff not directly employed) have their qualifications, experience and references etc. checked and corroborated as described in the "Certificate Manufacturer Procedures".

Similar checks on staff associated with the Registration Authorities are described in the Issuing Authority "Registration Authority Procedures".

5.3.2 BACKGROUND CHECK PROCEDURES

Background checks on all members of staff associated with the Certificate Manufacturer are carried out as described in the "Certificate Manufacturer Procedures".

Background checks on staff associated with the Registration Authorities are described in the Issuing Authority "Registration Authority Procedures".

5.3.3 TRAINING REQUIREMENTS

Appropriate training is provided to all members of staff associated with the Certificate Manufacture process as described in the "Certificate Manufacturer Procedures".

Appropriate training for staff associated with the Registration Authorities is described in the Issuing Authority "Registration Authority Procedures".

Training forms part of the process for certifying staff as authorised to conduct operational and trusted roles.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

Appropriate update training and retraining is provided to all members of staff associated with the Certificate Manufacturer as described in the "Certificate Manufacturer Procedures".

Appropriate retraining for staff associated with the Registration Authorities is described in the Issuing Authority "Registration Authority Procedures".

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

Members of staff associated with the Certificate Manufacturer are rotated between tasks as described in the "Certificate Manufacturer Procedures".

Staff responsible for the operation of the Registration Authorities are rotated as defined in the in the Issuing Authority "Registration Authority Procedures".

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

Unauthorised actions by members of staff are subject to formal personnel and Information System Security Management procedures. Details of the processes and sanctions are described in the "Certificate Manufacturer Procedures".

Irrespective of sanctions for particular events, authorisation to operate in an operational or trusted role can be withdrawn for any staff member at any time.

Unauthorised actions by staff responsible for the operation of Registration Authorities will result in sanctions as defined in the in the Issuing Authority "Registration Authority Procedures".

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

All contractors who operate within the Certificate Manufacturer are controlled and escorted as described in the "Certificate Manufacturer Procedures".

All contractors associated with the Registration Authorities are controlled as described in the Issuing Authority "Registration Authority Procedures".

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

Documentation is supplied in conformance with the governing Certificate Policy.

All members of staff associated with the Certificate Manufacturer are provided with all documentation relevant to their position; this includes the "Certificate Manufacturer Procedures".

All members of staff associated with the Registration Authorities are supplied with documentation as described in the Issuing Authority "Registration Authority Procedures".

5.4 AUDIT LOGGING PROCEDURES

5.4.1 TYPES OF EVENTS RECORDED

A range of specific events relating to the operation of a specific PKI are recorded to align with the relevant governing Certificate Policy. A range of key events are recorded for all systems.

Information on events recorded by the Certificate Manufacturer is given in the "Certificate Manufacturer Procedures".

Information on events recorded by the Registration Authorities is given in the Issuing Authority "Registration Authority Procedures".

5.4.2 FREQUENCY OF PROCESSING LOG

Processing of Audit Logs is controlled by the nature of items comprising the logs and any specific requirements of the governing Certificate Policy

The frequency at which Audit Logs are processed (and / or archived) by the Certificate Manufacturer is described in the "Certificate Manufacturer Procedures".

The frequency at which Audit Logs are processed (and / or archived) by the Registration Authorities is given in the Issuing Authority "Registration Authority Procedures".

5.4.3 RETENTION PERIOD FOR AUDIT LOG

The baseline minimum retention period for the Certificate Manufacturer audit logs is seven years.

The retention period for Registration Authorities audit logs is given in the Issuing Authority "Registration Authority Procedures".

5.4.4 PROTECTION OF AUDIT LOG

The procedures for the protection of Certificate Manufacturer audit logs are described in the "Certificate Manufacturer Procedures".

The procedures for the protection of Registration Authorities audit logs are described in the Issuing Authority "Registration Authority Procedures".

5.4.5 AUDIT LOG BACKUP PROCEDURES

The procedures for the backup of Certificate Manufacturer audit logs are described in the "Certificate Manufacturer Procedures".

The procedures for the backup of Registration Authorities audit logs are described in the Issuing Authority "Registration Authority Procedures".

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

In the case of the Certificate Manufacturer audit logs from both the underlying operating system and from the application software are recorded internally. A range of data recording measures are employed as described in the "Certificate Manufacturer Procedures". No external audit collection systems are used by the Certificate Manufacturer.

In the case of the Registration Authorities audit collection systems are described in the Issuing Authority "Registration Authority Procedures", this also describes whether they are internal or external.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

There is no statutory requirement to notify an End-Entity, organisation or other event causing entity.

Where significant events are considered security or policy relevant, the Certificate Manufacturer informs the Issuing Authority as described in the "Certificate Manufacturer Procedures"

The decision on the notification of events to the subject concerned is made by the Issuing Authority; this decision is implemented by the Registration Authority and carried out as described in the Issuing Authority "Registration Authority Procedures".

5.4.8 VULNERABILITY ASSESSMENTS

Regular risk and vulnerability assessments will be carried out on both the physical and logical infrastructure under the control of the Certificate Manufacturer. These will take place at regular intervals to support compliance audit. Additional assessments may be used where the Security Committee identifies an event, or a change to systems, which may have an impact on risks.

Vulnerability assessment requirements for any specific Registration Authority are prescribed by the Issuing Authority and these carried out as described in the Issuing Authority "Registration Authority Procedures".

5.5 RECORDS ARCHIVAL

A range of procedures are operated to ensure record archival complies with all governing Certificate Policies supported by the Certificate Manufacturer and using this CPS. In some cases, records are archived to fulfil the particular requirements of a specific governing Certificate Policy

5.5.1 TYPES OF RECORDS ARCHIVED

Information on the records that are archived by the Certificate Manufacturer is given in the "Certificate Manufacturer Procedures".

Information on the records that are archived by the Registration Authorities is given in the Issuing Authority "Registration Authority Procedures".

5.5.2 RETENTION PERIOD FOR ARCHIVE

The retention period for archived records is in conformance with the governing Certificate Policy.

The baseline minimum retention period Certificate Manufacturer archived records is seven years.

The retention period for Registration Authorities archived records is given in the Issuing Authority "Registration Authority Procedures".

5.5.3 PROTECTION OF ARCHIVE

Archive records are protected and controlled to the same standards as the original data.

The procedures for the protection of Certificate Manufacturer archived records are described in the "Certificate Manufacturer Procedures".

The procedures for the protection of Registration Authorities archived records are described in the Issuing Authority "Registration Authority Procedures".

5.5.4 ARCHIVE BACKUP PROCEDURES

The procedures for the backup of Certificate Manufacturer archived records are described in the "Certificate Manufacturer Procedures".

The procedures for the backup of Registration Authorities archived records are described in the Issuing Authority "Registration Authority Procedures".

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Records are time stamped in conformance with the governing Certificate Policy.

The Certificate Manufacturer obtains the current time for record time-stamping from a global verifiable source. Synchronisation and control of time used by the Certificate Manufacturer is conducted in accordance with the "Certificate Manufacturer Procedures".

The source of time used to time-stamp Registration Authorities records is selected by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

In the case of the Certificate Manufacturer the archive collection is performed internally. The process is described in the "Certificate Manufacturer Procedures". No external archive collection systems are used by the Certificate Manufacturer.

In the case of the Registration Authorities archive collection systems are described in the Issuing Authority "Registration Authority Procedures", this also describes whether they are internal or external.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

The procedures to obtain and verify archive information for the Certificate Manufacturer are described in the "Certificate Manufacturer Procedures".

The procedures to obtain and verify archive information for the Registration Authorities are described in the Issuing Authority "Registration Authority Procedures".

5.6 KEY CHANGEOVER

Key changeover requirements for each PKI are prescribed by the Issuing Authority in the relevant governing Certificate Policy.

All CA-Key management processes are subject to the Key splitting and management controls prescribed in the governing Certificate Policy. All Key changeover procedures strictly enforce the defined trust model for the relevant PKI. Certificate Status Information is maintained in accordance with Policy requirements until the CA-Key is expired or decommissioned and all subordinate End-Entity Certificates are no longer valid.

The procedures relating to Key changeover by the Certificate Manufacturer are described in the "Certificate Manufacturer Procedures".

For Registration Authorities Key change over must comply with the policy and trust model of the controlling Issuing Authority. Specific details are provided in Issuing Authority "Registration Authority Procedures".

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

The procedures by which the Certificate Manufacturer deals with incidents or the compromise of information are prescribed by the Security Management Committee and controlled via the Information Systems Management System (ISMS). Details are provided in the "Certificate Manufacturer Procedures".

The procedures by which the Registration Authorities deal with incidents or the compromise of information are described in the Issuing Authority "Registration Authority Procedures".

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

The Certificate Manufacturer business continuity strategy is designed to deal with any disruption to services. This is multi-level strategy to allow managed progressive recovery of components used to provide primary service and the alternative backup facilities. The Alternative Trust Service Centre, which represents the backup facility for major failure of primary systems, is geographically separate from the main operational site and has independent provision of power and other services. The Certificate Manufacturer Contingency Plan is described in the "Certificate Manufacturer Procedures". The Certificate Manufacturer Contingency Plan is reviewed and exercised, at a minimum, annually.

Business continuity for Registration Authorities is the responsibility of the Issuing Authority and is described in the Issuing Authority "Registration Authority Procedures".

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

The Certificate Manufacturer (or Certificate Authority) does not communicate with the Subscriber regarding Certificate or key related issues.

The obligation of Subscribers and the actions to be taken in such circumstances will be established by the Issuing Authority and published in the Subscriber Agreement associated with the governing Certificate Policy. Where procedures for End-Entity Private Key compromise involve action by Registration Authorities processes are described in the Issuing Authority "Registration Authority Procedures".

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

The Certificate Manufacturer business continuity strategy accommodates all circumstances up to and including a major disaster at the primary service provision location. The Certificate Manufacturer Contingency Plan incorporates transition to a backup facility located geographically separate from the main operational site. The Certificate Manufacturer Contingency Plan is described in the "Certificate Manufacturer Procedures". The Certificate Manufacturer Contingency Plan is reviewed and exercised at a minimum annually.

Business continuity for Registration Authorities is the responsibility of the Issuing Authority and is described in the Issuing Authority "Registration Authority Procedures".

5.8 CA OR RA TERMINATION

Termination procedures are designed to maintain conformance with the governing Certificate Policy.

Before ceasing to act as a Certificate Manufacturer, or terminating systems supporting an Issuing Authority and acting under a governing Certificate Policy, the Certificate Manufacturer will, at a minimum, undertake the following actions in the sequence as shown below:

1. Inform both the Issuing Authority and Policy Authority for the relevant governing Certificate Policy.
2. Establish a termination plan for the approval of the Policy Authority
3. In conjunction with the Policy Authority for the relevant governing Certificate Policy publish details of termination to Subscribers and Relying Parties.
4. Provide a notice period of 90 days.
5. Revoke all certificates at the end of 90 days if required by the Issuing Authority.
6. Arrange with a reliable third party (if required) for the preservation and storage of records for the minimum period of time stipulated for such preservation as required by the Issuing Authority but not less than 7 years.
7. Decommission CAs ensuring CA private keys are destroyed or remain protected at level commensurate at that for operational CAs.
8. Conduct any other actions as required by the governing Certificate Policy.

This process is documented in the "Certificate Manufacturer Procedures".

The process for the termination of Registration Authorities is dependent on specific scenarios. It all cases plans must be approved by the Policy Authority for the relevant governing Certificate Policy, even where there is no impact on the status of existing Certificates. Details of RA termination, where it is not part of the termination of a PKI Service or CA, shall be published by the Issuing Authority and/or Registration Authority.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

Private Keys are managed by a variety of mechanisms. All of which are designed to achieve security and integrity in order to ensure conformance with the governing Certificate Policy.

6.1.1 KEY PAIR GENERATION

Key pairs supporting infrastructure components used by the Certificate Manufacturer are generated as described in the "Certificate Manufacturer Procedures".

The Key pairs used by Registration Authorities and by Subscriber are generated as described in the Issuing Authority "Registration Authority Procedures".

The Issuing Authority defines and communicates requirements for End-Entity Key pair generation and management via the governing Certificate Policy and Subscriber Agreement.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

The Certificate Manufacture does not deliver Key pairs used for Digital Signatures. Services provided under this CPS always involve such Keys being generated locally to the Subscriber.

Where encryption Key pairs are created by a Participant other than the Subscriber, the mechanisms for delivery of Key pairs to Subscribers are described in the Issuing Authority "Registration Authority Procedures".

Where Cryptographic Tokens are involved they are distributed to Subscribers as described in the Issuing Authority "Registration Authority Procedures".

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

The delivery of Public Keys to the Certificate Manufacturer uses PKCS#10, other equivalent standards compliant cryptographic mechanism or using a process specifically approved by the Certificate Manufacturer. Specific mechanisms are defined by the Issuing Authority.

Where Subscriber Public Keys are delivered to the Certificate Manufacturer via Registration Authorities the mechanisms are described in the Issuing Authority "Registration Authority Procedures".

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

Whether the Issuing Authority provides CA Public Keys or delivery of same is devolved to the Certificate Manufacturer is defined by the Issuing Authority.

At a minimum the Certificate Manufacturer ensures all CA Public Keys relevant to a Trust Infrastructure are made available to Participants. Other Public Key dissemination is conducted as prescribed by the Issuing Authority.

A number of standard protocols are used for dissemination of Public Keys

6.1.5 KEY SIZES

Specific Key sizes are in conformance with the governing Certificate Policy.

CA-Keys are not less than 2048-bit modulus for RSA.

Subscriber's Key lengths are defined by the Issuing Authority and controlled by formal procedures for the management of Certificate Profiles implemented by the Certificate Manufacturer. Only the Certificate Manufacturer may implement or modify Certificate Profiles on behalf of the Issuing Authority.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

For Keys created and managed by the Certificate Manufacturer; Public Key parameter generation and checking is described in the "Certificate Manufacturer Procedures".

For Subscriber's Public Keys, parameter generation and checking is described in the Issuing Authority "Registration Authority Procedures".

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

Key usage is defined by the Issuing Authority and promulgated in the governing Certificate Policy.

The Certificate Manufacturer implements the Issuing Authority requirements through formal control procedures for Certificate Profile management.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

The Certificate Manufacturer (Certificate Authority) Keys are protected by the use of tamper resistant cryptographic modules (or hardware security modules) that comply at a minimum with FIPS 140-2 level 3 security engineering requirements. The controls applied to these modules are described in the "Certificate Manufacturer Physical Description" and "Certificate Manufacturer Procedures".

Cryptographic Modules used by Registration Authorities and Subscribers are defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Physical Description" and "Registration Authority Procedures".

Where specific cryptographic modules are required, the Issuing Authority defines the requirements in the governing Certificate Policy

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

Certain tasks such as those associated with the Certificate Manufacturer handling of Private Keys are performed under multi-person control using an “n out of m” approach. These are described in the “Certificate Manufacturer Procedures”.

See also Sections 4.12.1 and 5.2.2.

6.2.3 PRIVATE KEY ESCROW

Private Key escrow is not supported under this CPS.

6.2.4 PRIVATE KEY BACKUP

Private Key backup is in conformance with the governing Certificate Policy.

The Private Keys of the Certificate Manufacturer (Certificate Authority) are securely backed up as described in the “Certificate Manufacturer Procedures”. CA Private Keys are never available outside the cryptographic module in clear text form and are protected by the “n out of m” control mechanism (ref. Section 6.2.2)

The backup of Private Keys relating to Registration Authorities is defined by the Issuing Authority and described in the Issuing Authority “Registration Authority Procedures”.

6.2.5 PRIVATE KEY ARCHIVAL

The Private Keys of the Certificate Manufacturer (Certificate Authority) are securely archived as described in the “Certificate Manufacturer Procedures”. CA Private Keys are never available outside the cryptographic module in clear text form and are protected by the “n out of m” control mechanism (ref. Section 6.2.2)

The archive of Private Keys relating to Registration Authorities is defined by the Issuing Authority and described in the Issuing Authority “Registration Authority Procedures”.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

The transfer in to and from cryptographic modules of the Private Keys of the Certificate Manufacturer (Certificate Authority) is described in the “Certificate Manufacturer Procedures”. CA Private Keys are never available outside the cryptographic module in clear text form and are protected by the “n out of m” control mechanism (see Section 6.2.2)

The transfer in to and from cryptographic modules of the Private Keys used by Registration Authorities and Subscribers are defined by the Issuing Authority and described in the Issuing Authority “Registration Authority Procedures”.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

Private Key storage in cryptographic modules is in conformance with the governing Certificate Policy.

The storage of Keys in cryptographic modules of the Certificate Manufacturer (Certificate Authority) is described in the "Certificate Manufacturer Procedures". CA Private Keys are never available outside the cryptographic module in clear text form and recovery is protected by the "n out of m" control mechanism (ref. Section 6.2.2)

The storage of Keys used by Registration Authorities and Subscribers is defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

A number of mechanisms for activation of Private Keys are used to ensure compliance with governing Certificate Policy.

The activation of the Keys in the cryptographic modules used by the Certificate Manufacturer (Certificate Authority) is described in the "Certificate Manufacturer Procedures" (ref. Section 6.2.2)

The activation of Keys used by Registration Authorities and Subscribers is defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

A number of mechanisms for deactivation of Private Keys are used to ensure compliance with governing Certificate Policy.

The deactivation of the Keys in the cryptographic modules used by the Certificate Manufacturer (Certificate Authority) is described in the "Certificate Manufacturer Procedures" (ref. Section 6.2.2)

The deactivation of Keys used by Registration Authorities and Subscribers is defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".

6.2.10 METHOD OF DESTROYING PRIVATE KEY

Strict controls are implemented over Private Key destruction to ensure compliance with the governing Certificate Policy.

The destruction of the Keys in the cryptographic modules used by the Certificate Manufacturer (Certificate Authority) is described in the "Certificate Manufacturer Procedures" (ref. Section 6.2.2)

The destruction of Keys used by Registration Authorities and Subscribers is defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".

6.2.11 CRYPTOGRAPHIC MODULE RATING

Cryptographic modules are in conformance with the governing Certificate Policy. Only cryptographic modules which are assessed and rated to accepted international standards are employed.

The Certificate Manufacturer (Certificate Authority) uses tamper resistant cryptographic modules (or Hardware Security Modules) that comply with FIPS 140-2 level 3 security engineering requirements.

Cryptographic Modules used by Registration Authorities and Subscribers are defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Physical Description" and "Registration Authority Procedures".

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

The archiving of Public Keys, and other backup related activities, by the Certificate Manufacturer are described in the "Certificate Manufacturer Procedures".

The archiving of Public Keys, and other backup related activities, by the Registration Authorities are defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".

Any specific requirements for Subscriber Public Key archiving by End Entities are defined by the Issuing Authority and promulgated in the governing Certificate Policy and Subscriber Agreement.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

Certificate operational periods and Key Pair usage periods are specified in the governing Certificate Policy.

The Certificate Manufacturer implements the Issuing Authority requirements through formal control procedures for Certificate Profile management.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

Activation data relating to Certificate Manufacturer Private Keys and cryptographic modules is securely generated and protected, for example Private Keys are never available outside the cryptographic module in clear text form and are protected by the "n out of m" control mechanism (ref. Section 6.2.2). The associated Certificate Manufacturer processes are described in the "Certificate Manufacturer Procedures".

A range of mechanisms and standards are employed to ensure security controls on the activation of Subscriber's Keys, and security devices that hold or control Subscriber's Keys.

For Registration Authorities and Subscribers, the activation data requirements are defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".

6.4.2 ACTIVATION DATA PROTECTION

Activation data relating to Certificate Manufacturer held CA-Keys and associated cryptographic modules is protected as described in the "Certificate Manufacturer Procedures". Distribution of Key shares is defined by the Issuing Authority and agreed between the Issuing Authority and Certificate Manufacturer and / or other Participants authorised to hold Key shares.

In the case of Registration Authorities and Subscribers the steps to be taken to protect activation data are defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures" and / or Subscriber Agreement.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

All other aspects of activation data relating to Certificate Manufacturer Private Keys and cryptographic modules is described in the "Certificate Manufacturer Procedures".

In the case of Registration Authorities and Subscribers all other aspects of activation data are defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

Computer security technical measures are in conformance with the governing Certificate Policy.

Specific security functionality relating to the Certificate Manufacturer is described in the "Certificate Manufacturer Physical Description" and "Certificate Manufacturer Procedures".

Specific security functionality relating to the Registration Authorities is described in the Issuing Authority "Registration Authority Physical Description" and "Registration Authority Procedures".

6.5.2 COMPUTER SECURITY RATING

Individual components of the Certificate Manufacturer operational environment have ITSEC, FIPS or Common Criteria security ratings. The Certificate Manufacturer as a whole has been reviewed and holds a number on industry recognised accreditations and certifications. (The Certificate Manufacturer web site should be accessed for the current list of these).

The security rating and accreditations of the operational environment for Registration Authorities may be obtained from the Issuing Authority.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

The Certificate Manufacturer does not conduct software development of security enforcing CA Systems. The Certificate Manufacturer uses a number of established products from a range of suppliers. Such products, where appropriate, carry accreditations and certifications applicable to their role and required assurance levels.

The configuration of the operational systems built from these standard products is managed in compliance with ISO 27001 and subject to external audit and approval. Details are provided in the "Certificate Manufacturer Procedures". The quality system used by the Certificate Manufacturer is ISO9001 compliant and is described in the "Certificate Manufacturer Procedures".

The development associated with Registration Authorities is managed by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".

All products and aspects of Registration Authority implementation are evaluated as compliant with the governing Certificate Policy by the Certificate Manufacturer prior to connection and interaction with any systems operated by the Certificate Manufacturer.

6.6.2 SECURITY MANAGEMENT CONTROLS

The Certificate Manufacturer's Security Committee has responsibility for all Security Management activities. Security and its management is conducted in compliance with ISO 27001 and is subject to external audit and approval. Details of Security Management controls are described in the "Certificate Manufacturer Procedures".

The Security Management controls associated with Registration Authorities are defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".

Security of Registration Authority implementations are evaluated as compliant with the governing Certificate Policy by the Certificate Manufacturer prior to connection and interaction with any systems operated by the Certificate Manufacturer.

6.6.3 LIFE CYCLE SECURITY CONTROLS

The life cycle controls used by the Certificate Manufacturer are described in the "Certificate Manufacturer Procedures".

The life cycle controls associated with Registration Authorities are defined by the Issuing Authority and described in the Issuing Authority "Registration Authority Procedures".

6.7 NETWORK SECURITY CONTROLS

The network security controls in use within the Certificate Manufacturing facility consist of a combination of security products and appropriate network monitoring, control and operating procedures. These controls are described in the "Certificate Manufacturer Facility Physical Description" and "Certificate Manufacturer Procedures".

The network security associated with Registration Authorities is described in the Issuing Authority "Registration Authority Procedures.

6.8 TIME-STAMPING

Time Stamping is conducted as an integral component of Certificate Manufacturer operations for all Certificate and other related activities that require recorded time. A global verifiable time source is used. Synchronisation and control of time used by the Certificate Manufacturer is conducted in accordance with the "Certificate Manufacturer Procedures" (See also Section 5.5.5).

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Certificate Profiles are used to define and control parameters embodied into Certificates issued.

All aspects of Certificate Profile development and implementation are conducted by the Certificate Manufacturer on behalf of the Issuing Authority who defines the profiles for Certificates and Certificate Status information.

Certificate Profiles are strictly managed to ensure compliance with the governing Certificate Policy

7.1.1 VERSION NUMBER(S)

Certificates conforming to X.509 version 3 are supported.

7.1.2 CERTIFICATE EXTENSIONS

Certificate Profiles are defined in conjunction with the Issuing Authority as described in the "Certificate Manufacturer Procedures". The following certificate extensions are commonly employed:

- The Basic constraints extension is included in all certificates issued under this CPS.
- Subscriber Certificates have the CA element set to false, CA-Certificates have the CA element set to true
- The Certificate Policy Qualifier Info extension is included.
- Where CRLs are used to produce Certificate Status Information, the CRL Distribution Point extension is included.

All certificate extension use is subject to approval by the Issuing Authority.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

Certificate Profiles are defined in conjunction with the Issuing Authority as described in the “Certificate Manufacturer Procedures”.

7.1.4 NAME FORMS

Certificate Profiles are defined in conjunction with the Issuing Authority as described in the “Certificate Manufacturer Procedures”.

7.1.5 NAME CONSTRAINTS

Certificate Profiles are defined in conjunction with the Issuing Authority as described in the “Certificate Manufacturer Procedures”.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

Certificate Policy object identifiers are used as specified in the governing Certificate Policy.

The Certificate Policy Object Identifier extension is included in all certificates and references the governing Certificate Policy.

Certificate Profiles are defined in conjunction with the Issuing Authority as described in the “Certificate Manufacturer Procedures”.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

Certificate Profiles are defined in conjunction with the Issuing Authority as described in the “Certificate Manufacturer Procedures”.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

Certificate Profiles are defined in conjunction with the Issuing Authority as described in the “Certificate Manufacturer Procedures”.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

Not applicable to this CPS.

7.2 CRL PROFILE

All aspects of CRL profile development and implementation are conducted by the Certificate Manufacturer on behalf of the Issuing Authority who defines the profiles for CRLs and Certificate Status Information.

CRL profiles are strictly managed to ensure compliance with the governing Certificate Policy

7.2.1 VERSION NUMBER(S)

Certificate Revocation Lists conforming to X.509 version 2 are supported.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

The use of CRL and CRL Entry Extensions is described in the "Certificate Manufacturer Procedures".

7.3 OCSP PROFILE

All aspects of OCSP profile development and implementation are conducted by the Certificate Manufacturer on behalf of the Issuing Authority who defines the profiles for OCSP and other Certificate Status information.

OCSP profiles and protocols are strictly managed to ensure compliance with the governing Certificate Policy.

7.3.1 VERSION NUMBER(S)

See Section 7.3.

7.3.2 OCSP EXTENSIONS

See Section 7.3.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

An external assessment of the Certificate Manufacturer is performed twice yearly (this activity supports its industry recognised accreditations and certifications – ref. Section 6.5.2). This external assessment is performed by organisations that hold relevant accreditation to perform this activity. The findings of the assessment are provided to the Policy Authority. Additional audit assessments of some or all of the Certificate Manufacturer operations may be undertaken.

Internal audit assessments are performed annually. These include a range of routine checks and audit activities which are reported to the Security Management Committee.

Assessment of the Issuing Authority and its associated Registration Authorities is decided by the Issuing Authority. Registration Authority implementations are evaluated as compliant with the governing Certificate Policy by the Certificate Manufacturer prior to connection and interaction with any systems operated by the Certificate Manufacturer.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The external assessors for the Certificate Manufacturer are selected from those that hold relevant industry recognised accreditations and certifications for the scheme under which the assessment is performed. Internal audit is performed by suitably qualified and approved staff with applicable training and experience.

The suitability of assessors to perform assessment of the Certificate Manufacturer is decided by the Policy Authority.

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

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The relationship between the assessor and the Certificate Manufacturer will depend on whether an external or internal assessment (audit) is being performed:

- External assessor – must have no relationship with the Certificate Manufacturer other than a contractual one covering the assessments.
- Internal Audit – there are no restrictions on the auditor's relationship to the Certificate Manufacturer but the auditor must demonstrate adequate independence from the audited party.

The determination of acceptability of the relationship between the assessors and the Issuing Authority will be decided by the Policy Authority.

8.4 TOPICS COVERED BY ASSESSMENT

In the case of the external assessments the topics covered and the scope of the assessment are defined by the organisations responsible for the management of the particular scheme under which assessment is sought. In the case of internal audit, the topics to be covered will be defined by the Security Committee and / or Quality Committee.

In the case of the assessment of the Issuing Authority and its associated Registration Authorities the scope of the assessment will be decided by the Issuing Authority and agreed to by the Policy Authority.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The actions that are taken as a result of any deficiencies that are identified during the assessment of the Certificate Manufacturer services will depend on the seriousness of the deficiency and its potential impact. The Policy Authority has the overall responsibility for deciding what actions are to be taken. The Certificate Manufacturer informs the Issuing Authority of all significant reported deficiencies whether identified by internal or external audit. The decision on action to be taken will be based on a

variety of factors including previous responses to deficiencies, the severity of the deficiency and the recommendations of the assessor.

In the case that deficiencies are identified during the assessment of the Issuing Authority and its associated Registration Authorities, responsibility for deciding what actions are to be taken lies with the Issuing Authority, who must inform the Policy Authority of all significant deficiencies.

The Policy Authority has ultimate authority upon remedial actions taken following identification of deficiencies.

8.6 COMMUNICATION OF RESULTS

The results of the assessment of the Certificate Manufacturer services are in the first instance communicated to the Policy Authority. The Policy Authority is responsible for communicating relevant information from the assessment results to other Participants as is appropriate.

The results of the assessment of the Issuing Authority and its associated Registration Authorities are in the first instance communicated to the Issuing Authority. The Issuing Authority is responsible for informing the Policy Authority of the results of assessment.

The Policy Authority is responsible for communicating relevant information from the assessment results to other Participants as is appropriate.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

Any fees charged by the Certificate Manufacturer are as specified in the contracts between the Certificate Manufacturer and the Issuing Authority.

Fees charged to Subscribers are the responsibility of the Issuing Authority.

9.1.2 CERTIFICATE ACCESS FEES

Any fees charged by the Certificate Manufacturer are as specified in the contracts between the Certificate Manufacturer and the Issuing Authority.

Fees charged to Subscribers or other End-Entities are the responsibility of the Issuing Authority.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

Any fees charged by the Certificate Manufacturer are as specified in the contracts between the Certificate Manufacturer and the Issuing Authority.

Fees charged to Subscribers or other End-Entities are the responsibility of the Issuing Authority

9.1.4 FEES FOR OTHER SERVICES

Any fees charged by the Certificate Manufacturer are as specified in the contracts between the Certificate Manufacturer and the Issuing Authority.

Fees charged to Subscribers or other End-Entities are the responsibility of the Issuing Authority

9.1.5 REFUND POLICY

Any refund policy for the Certificate Manufacturer is as specified in the contracts between the Certificate Manufacturer and the Issuing Authority.

The refund policy to Subscribers is the responsibility of the Issuing Authority. If applicable, details of refunds will be provided in the Subscriber or Relying Party Agreements

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

The Certificate Manufacturer maintains insurance coverage for its liabilities to other Participants in the certificate issuance process. The level of insurance is specified in the contracts between the Certificate Manufacturer and the Issuing Authority.

The Issuing Authority is responsible for ensuring that it maintains mechanisms to cover its liabilities to other Participants in the Certificate issuance process (notably the Registration Authorities) and for its Liability to End-Entities.

9.2.2 OTHER ASSETS

The Certificate Manufacturer and other Participants providing Trust Services may have access to other resources to support operations and pay damages for potential liability to other participants in the certificate issuance process. These assets are specified as required in the contracts between the Participant and the Issuing Authority.

The Issuing Authority is responsible for ensuring that it has access to resources to support operations and pay damages for potential liability to other Participants and to End-Entities.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

Participants providing trust services do not provide any insurance or warranty coverage for End-Entities, whose contractual relationship is with the Issuing Authority.

The Issuing Authority is responsible for ensuring adequate mechanisms to support any warranty or other liabilities to End-Entities.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

All personal and corporate information obtained by the Certificate Manufacturer from the Issuing Authority, Registration Authorities or End Entities, which does not appear in Certificates or Certificate Status Information, is treated as Confidential.

Private Keys, CA-Keys and access control information for them are treated by the Certificate Manufacturer as Confidential. The “reason for revocation” of a certificate is also treated as Confidential. (Note: The Certificate Manufacturer does not hold or have access to the Private Keys of End Entities.)

Any information that contains personal and / or corporate information obtained by the Certificate Manufacturer as part of providing services (such as system logs, audit reports etc.) is treated as Confidential.

Confidential 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 considered confidential unless special agreements with the Issuing Authority so dictate.

Identification information and other personal or corporate information appearing in Certificates is not considered Confidential by the Certificate Manufacturer unless special agreements with the Issuing Authority so dictate.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

The Certificate Manufacturer maintains the confidentiality of information in conformance with the provisions of the governing Certificate Policy. All Confidential material is protected under the Certificate Manufacturer security policies at a classification level of "Confidential", these security policies are described in the “Certificate Manufacturer Procedures”. The information security policies are audited to ensure that they, at a minimum, comply with the agreements made with the Issuing Authority and the relevant governing Certificate Policies.

The Issuing Authority is responsible for the protection of Confidential information it, Registration Authorities or other Participants hold.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

The Certificate Manufacturer operates in conformance with the current UK legislation relating to Privacy and Data Protection and in accordance with the contractual relationship with the Issuing Authority.

The Issuing Authority is responsible for ensuring that both it and the entities under its control have in place an appropriate privacy plan.

9.4.2 INFORMATION TREATED AS PRIVATE

All personal and corporate information obtained by the Certificate Manufacturer from the Issuing Authority, Registration Authorities or End Entities, which does not appear in Certificates or Certificate Status Information, is treated as private.

Any information that contains personal and / or corporate information obtained by the Certificate Manufacturer as part of providing services is treated as Confidential.

The “reason for revocation” of a Certificate is also treated as private.

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

9.4.3 INFORMATION NOT DEEMED PRIVATE

Certificates, Certificate Status, and the data contained therein are not considered private unless special agreements with the Issuing Authority so dictate. Identification information or other personal or corporate information appearing in Certificates is not treated as private by the Certificate Manufacturer unless special agreements with the Issuing Authority so dictate.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

The Certificate Manufacturer maintains the privacy of information in conformance with the provisions of the governing Certificate Policy and applicable current legislation. All private material is protected under the Certificate Manufacturer security policy at a classification level of "Confidential", these security policies are described in the “Certificate Manufacturer Procedures”. These information security policies are audited to ensure that they, at a minimum, comply with the agreements made with the Issuing Authority.

The Issuing Authority is responsible for the protection of private information it or the Registration Authorities hold.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

The Certificate Manufacturer operates in conformance with the current legislation relating to Privacy and Data Protection and in accordance with the contractual relationship with the Issuing Authority.

The Issuing Authority is responsible for ensuring that it and all Participants have in place appropriate procedures and mechanisms to comply with applicable current legislation.

This is established via contractual arrangements with Participants together with direct communication of requirements via End-Entity Agreements or associated privacy declarations.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

Information shall be disclosed by the Certificate Manufacturer 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 which it is lawfully obligated to disclose.

The Issuing Authority is responsible for the disclosure of private information it or the Registration Authorities hold under the same circumstances.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Information held by the Certificate Manufacturer may also be disclosed:

- On the owner's request, to facilitate such disclosure an authenticated request from the information owner must be provided prior to the release of the information.
- At the specific request of the Policy Authority (in so far as permissible by current applicable legislation.)

The Issuing Authority is responsible for the disclosure of private information it or Registration Authorities hold.

9.5 INTELLECTUAL PROPERTY RIGHTS

All copyright and other intellectual property rights in this Certification Practice Statement ('the Materials'), provided or made available by Entrust (Europe) Ltd, shall remain the property of Entrust (Europe) Ltd. Entrust (Europe) Ltd grants the Policy Authority and those Trust Service Providers (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, this 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) Ltd is an approved Trust Service Provider.

Participants, Subscribers, Relying Parties 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 Certification Practice Statement they will do nothing illegal or in infringement of any third party rights and in particular will ensure that any material that they supply or transmit is not illegal, libelous, and does not infringe any intellectual property right.

9.6 REPRESENTATIONS AND WARRANTIES

The Issuing Authority is the only Participant that provides warranties direct to End Entities. Other Participants maintain a relationship with the Issuing Authority only.

9.6.1 CA REPRESENTATIONS AND WARRANTIES

Certificate Manufacturer representations and warranties are defined in the contract with the Issuing Authority.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

Registration Authority representations and warranties are defined in the contract with the Issuing Authority.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

Subscriber representations and warranties are defined by the Issuing Authority and published in the governing Certificate Policy and Subscriber Agreement

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

Relying Party representations and warranties are defined by the Issuing Authority and published in the governing Certificate Policy and Relying Party Agreement.

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

Representations and warranties relating to other Participants are defined by the Issuing Authority and published in the governing Certificate Policy or are part of contractual arrangements with the Issuing Authority.

9.7 DISCLAIMERS OF WARRANTIES

The requirement for disclaimers of express warranties that may otherwise be deemed to exist in an agreement, and disclaimers of implied warranties that may otherwise be imposed by applicable law, such as warranties of merchantability or fitness for a particular purpose will be incorporated into the contract between the Participants providing Trust Services and the Issuing Authority.

9.8 LIMITATIONS OF LIABILITY

The Certificate Manufacturer and Participants providing Trust Services limits any liability (other than that arising from death or personal injury as a result of its negligence) for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon Certificates or associated Public / Private Key pairs issued under this Certification Practice Statement, to that defined by the governing Certificates Policies under which the Certificate Practice Statement operates.

The Certificate Manufacturer and Participants providing Trust Services accept no liability (other than that arising from death or personal injury as a result of its negligence, or fraudulent misrepresentation) in relation to Certificates and their use by End Entities and does not accept any direct liability to others including Subscribers and Relying Parties.

Participants providing Trust Services are liable only to the Issuing Authority for the functions they undertake on its behalf. The liabilities of Participants providing Trust Services are governed by the contract between the Certificate Manufacturer and the Issuing Authority.

9.9 INDEMNITIES

Any relevant indemnities will be incorporated into the contract between the Participants providing Trust Services and the Issuing Authority.

The Issuing Authority may require indemnities of Participants and others. Where applicable, indemnity requirements are specified in Contracts between the Issuing Authority and Participants. These include but are not limited to governing Certificate Policy, Subscriber and Relying Party Agreements.

9.10 TERM AND TERMINATION

9.10.1 TERM

The contracts between the Participants providing Trust Services and the Issuing Authority defines the term of a document or agreement, that is, when the document becomes effective and when it expires if it is not terminated earlier".

The contractual commitment between Subscribers, Relying Parties and the Issuing Authority may be defined in the governing Certificate Policy. The applicable Certificate Policy remains in force at all times when a Certificate has a status which is valid.

9.10.2 TERMINATION

The contracts between the Participants providing Trust Services and the Issuing Authority defines the termination provisions stating circumstances under which the document, certain portions of it, or its application to a particular participant ceases to remain in effect.

These termination procedures are in conformance with the governing Certificate Policy.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

This CPS shall be binding upon, and injure to the benefit of all parties hereto. The rights and obligations detailed in this CPS are not assignable by the parties without the others consent and any purported assignment without such shall be void.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Communications between the Participants providing Trust Services and the Issuing Authority (and the Policy Authority) will be agreed between the parties (and in conformance with the governing Certificate Policy).

Communication with the other parties, including Registration Authorities and Subscribers, is defined by the Issuing Authority and published in the governing Certificate Policy.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

Amendments to this CPS fall into three categories:

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

Where the amendments are likely to have a major impact on the majority of users of this CPS 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 CPS will be notified in writing to those Issuing Authorities that are registered with the Policy Authority.

Impacted users may file comments with 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 the Subscribers or Relying Parties using this CPS 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 CPS 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 at the sole 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.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

Not Applicable.

9.13 DISPUTE RESOLUTION PROVISIONS

All disputes shall be referred by the Issuing Authority in writing to the Policy Authority. The Policy Authority shall deal with such disputes in accordance with the governing Certificate Policy and the relevant contracts between the Issuing Authority and Participants.

Participants shall refer disputes to the relevant Issuing Authority that is responsible for their resolution or for their escalation to the Policy Authority as described above.

9.14 GOVERNING LAW

This CPS shall be governed by the law of England and Wales and the parties submit to the exclusive jurisdiction of the courts of England and Wales and this contract is deemed to be made in England and Wales.

9.15 COMPLIANCE WITH APPLICABLE LAW

All Participants within the PKI will comply with all applicable law and regulations, for example (but not limited to) Data Protection, those items of cryptographic hardware and software that subject to export controls, access by law enforcement.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

Not Applicable.

9.16.2 ASSIGNMENT

This CPS shall be binding upon, and injure to the benefit of all parties hereto. The rights and obligations detailed in this CPS are not assignable by the parties without the others consent and any purported assignment without such shall be void.

9.16.3 SEVERABILITY

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

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

Not Applicable.

9.16.5 FORCE MAJEURE

The Certificate Manufacturer and Participants providing Trust Services shall have no liability to the Issuing Authority or other Participants operating under this CPS if they are prevented from or delayed in performing its obligations under this CPS, 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.

9.17 OTHER PROVISIONS

9.17.1 FIDUCIARY RELATIONSHIPS

Issuance of Certificates does not make the Issuing Authority or any Participant Providing Trust Services a fiduciary, trustee, or other representative of Subscribers or Relying Parties.

Capitalisation is used throughout this document for referencing defined terms, with the exception of Section Headings which have been retained in the format compliant with RFC 3647.