UTSP

Part of pay.uk

UTSP Certificate Policy

Document Version Control			
Version	Date	Author	Changes
0.15	08-11-2018	Tom Jerrard	Original Document
0.16	03-03-2020	Praveen Jain	UTSP (Part of pay.UK) logo updated

UTSP

CERTIFICATE POLICY

1 INTRODUCTION

All capitalised words have the meaning given in the DEFINITIONS document available at http://utsp.trustis.com/.

1.1 Overview

This UTSP Certificate Policy is drafted in accordance with X.509 standard RFC 3647 and consists of the following:

Title	Purpose	Reference
Definitions	This document defines key terms that are used in the Certificate Policy or in a Certificate Document.	http://utsp.trustis.com/
(UTSP) Certificate Policy	This is the main document that sets out the terms and conditions or policies governing the Issuance of and or management of (UTSP) Digital Certificates and the respective obligations of parties or individuals that Rely on or use these Certificates. It is supplemented by documents that are referenced herein (each a "Certificate Document").	**This document**
The Relying Party Agreement	These terms apply to and must be accepted by each party that is Relying upon a Certificate or the information embedded in a Certificate or is accessing or using Certificate Status Information.	http://utsp.trustis.com/
The Certificate Subscriber Agreement	Certificate Subscribers must comply with and are required to promulgate these terms to all Relevant Parties or Certificate Subjects in order to flow down terms of the Certificate Policy that govern Issuance of and management of Certificates and associated Private Keys. Further the Certificate Subscriber or an authorised representative acting on behalf of the Certificate Subscriber is required to accept these terms on behalf of a Subject that is identified in the	http://utsp.trustis.com/

	Certificate.	
The Certificate Subject Agreement	This is an agreement between the Certificate Subscriber and a Certificate Subject that establishes the rights and responsibilities of the parties regarding the issuance and management of Certificates and associated Private Keys.	This document
Privacy Policy	These privacy terms apply to and govern the use of Personal Data that is supplied by any individual whether as a Subject or as a Relevant Party (REP) as defined in section 1.1.3 or on behalf of their respective individual user(s) or such data that is supplied by any third party 'information source' at the request of a REP, an Issuing Authority, a Registration Authority or a Policy Authority for the purpose of providing or accessing the Trust Service.	http://utsp.trustis.com/

1.1.1 The UTSP Trust Service

The Trust Service provided by UTSP implements a closed Public Key Infrastructure in the sense that access and participation is only open to those who both satisfy eligibility criteria and are approved by UTSP. The Parties who are eligible to receive the Trust Service from UTSP including those providing trust services internally within their organisation and End-Entities authorised and approved to Issue, obtain, use, and/or Rely upon Certificates that reference this Certificate Policy are defined in this Certificate Policy. Participation is conditional upon agreeing to be bound by the terms of this Certificate Policy. Any use of a Certificate must be supported by the use of strong cryptography and highly robust registration mechanisms to a defined and assured level of trust and security.

1.1.2 Certificate use

Certificates issued under this Certificate Policy may only be used for the following purposes:

i. Authenticated access to UK payment or payment related systems of Pay.UK Limited including but not limited to the services of The Payment Schemes.

ii. Digital signing of payment transactions and payment files and other submissions to the Payments Schemes’ Central Infrastructure provider(s) by Payment Scheme participants and their authorised customers.

iii. Digital signing of data to be sent by the Payments Schemes’ Central Infrastructure provider(s) to Payment Scheme participants.

1.1.2.1 Certificate type, validation procedures and terms of usage

Applicants for Certificates are required to submit to the validation of identity credentials and their eligibility to hold such a Certificate in accordance with Participant's Enrolment Procedures.

1.1.2.2 Certificate Status Information

Certificate Status Information confirming the validity of a Certificate is updated every 2 - 2½ hours and immediately upon revocation through the generation of a new CRL. The Certificate Status information is made available via a Trustis OCSP Service. The OCSP service location is identified via an AIA entry in Subscriber's Certificate(s).

1.1.3 Who needs to comply with the Certificate Policy?

Any person, party, entity or device that applies for, uses or Relies on a UTSP Digital Certificate needs to comply with this Certificate Policy. Further the Issuing Authority (and its supplier Trustis Limited) has an obligation to operate a PKI in accordance with this Certificate Policy.

Each party that is participating in a PKI including a Certificate Subscriber (including Participants and where relevant their Customers and Suppliers), Certificate User, Relying Party and any other party identified in Section 1.3 below *(each referred to as a "Relevant Party" or "REP" in this document)* is responsible for observing the terms of this Certificate Policy and for administering or flowing through these terms to a party (including to another REP) or their respective individual users to the extent such party or individual is involved in an activity of Relying or using a UTSP Digital Certificate.

The Certificate Policy and its terms shall form a binding agreement between (i) a REP and another REP (if that is the case); and or (ii) a REP and its respective individual users. Further in either case each party shall require the other party to flow down these terms to their respective individual users

Who is responsible for accepting and ensuring that the Certificate Policy terms including the Certificate Subject Agreement are met?

	Participant	**Customer/Supplier**	**Natural person subject or person managing an app/device.**
CP	Accepts term of CP via UTSP Participant contract (UTSP Trust Service Participant Agreement or UTSP RtP Heads of Terms Agreement)	Accepts terms of CP via Banking or Supplier or Participant	
Certificate Subscriber Agreement	Accepts terms of Certificate Subscriber Agreement via UTSP Participant contract	Accepts terms of Certificate Subscriber Agreement via Banking or Supplier or Participant	
Certificate Subject Agreement			Accepts terms of Certificate Subject Agreement via employer (Customer/Supplier).

1.1.4 What is a Certificate Policy?

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

This Certificate Policy is structured according to the guidelines provided by IETF RFC 3647 with extensions and modifications defined where appropriate. It defines a Public Key Infrastructure and specifies:

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

1.2 Document name and identification

This policy document is registered by Trustis operating in an authorised administrative role for the Policy Authority and Issuing Authority defined below. Trustis is registered with the Internet Address Naming Authority (IANA) and has been assigned an object identifier ("OID") of 1.3.6.1.4.1.5237.

1.2.1 Identification of this Certificate Policy:

All Certificates issued under this Certificate Policy with the exception of Certificates issued for the RtP Service have been assigned an Object Identifier (OID) of 1.3.6.1.4.1.5237.131.1.1.

All Certificates issued under this Certificate Policy for the RtP Service have been assigned an Object Identifier (OID) of 1.3.6.1.4.1.5237.131.1.2.

1.3 Parties in the PKI Trust Service

1.3.1 Overview of the Parties

The Issuing Authority does not conduct all aspects of PKI operations itself. There are sets of functions that are delegated to Trustis or to Participants.

Parties who are participating in a PKI may perform one or more roles in any particular PKI. Typically these roles are:-

- Policy Authority
- Trust Service Providers
  - Certification Authority: Issuing Authority (UTSP) and Certificate Manufacturer (Trustis) Registration Authority (UTSP)
  - Local Registration Authority (LRA)
  - Repository (Trustis and UTSP)
- End Entities who use Certificates

- Participant and where applicable their Customers and Suppliers (all Certificate Subscribers)
- Certificate Subject
- Relying Party

Further the requirements placed upon each party providing Trust Services which support the Issuing Authority are controlled by the provisions of this Certificate Policy and the contractual arrangements between them and the Issuing Authority including:

- The Trustis Service Contract
- The UTSP Trust Service Participant Agreement
- The UTSP RtP Heads of Terms Agreement
- The Subscriber Agreement(s)
- The Certificate Subject Agreement(s)
- The Relying Party Agreement(s)
- The Privacy Policy

For the avoidance of doubt where Subjects hold Certificates on behalf of Certificate Subscribers in all such cases the contractual relationship with the Issuing Authority is/are held by the Participant and where necessary the obligations are flowed through to the Participant's Customers and Suppliers.

The Policy Authority has overall and final control over the content of the Certificate Policy and related documentation.

1.3.2 Certification Authorities

RFC 3647 defines Certification Authorities as the entities that Issue Certificates. Within the scope of the model outlined a "Certification Authority" consists of the two elements described in 1.3.3 Issuing Authority (UTSP) and 1.3.4 Certificate Manufacturer (Trustis).

1.3.3 Issuing Authority

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

The Issuing Authority is UTSP Limited.

The Issuing Authority supported by the Trustis Service has the ultimate responsibility for deciding the requirements that need to be fulfilled for the issue of a Certificate carrying its name as the Issuer. Irrespective of whether PKI services are provided by internal resources or are contracted out to external parties, the provisions of this Certificate Policy shall apply. The terms of the Certificate Policy are complemented by terms of the relevant contracts between the Issuing Authority and the parties supporting or providing Trust Services (as more specifically set out in Section 1.3.1 above) and all such agreements are collectively referred to as the Trust Service Terms.

The Issuing Authority is to ensure that all Certificates issued under this Certificate Policy contain a reference to where this Certificate Policy document is published. This is achieved by the Trustis Service Contract.

The Issuing Authority has defined a number of business processes that are to be incorporated by Participants in their standard operating procedures. These are made available to Participants. Throughout this document these business processes are referred to as the Issuing Authority "Registration Policy and Procedures".

Contact details:

UTSP Issuing Authority

Mailing Address:
UTSP Limited,
2 Thomas More Square,
London,
E1W 1YN,
UK
Email: UTSP@wearepay.uk

1.3.3.1 Reliance Limits

1.3.3.2 Reliance limits may be set by applicable law or by agreement

1.3.3.3 Limited Warranty & Disclaimer/Limitation of Liability

Warranties and limitations of liability are devolved to the contractual arrangements between the parties involved in the Trust Service.

1.3.3.4 Applicable Agreements, Certification Practice Statement, Certificate Policy

Copies of the Certificate Policy, Certificate Subscriber Agreement, Certificate Subject Agreement, Relying Party Agreement and the Definitions document that are updated from time to time are published by the Issuing Authority at http://utsp.trustis.com/.

The Certification Practice Statement is confidential to Trustis and UTSP.

1.3.3.5 Privacy Policy

The Privacy Policy is available at http://utsp.trustis.com/.This document may be updated from time to time.

1.3.3.6 Refund Policy

The UTSP Issuing Authority does not provide refunds for issued Certificates.

1.3.3.7 Dispute Resolution:

Disputes between Participants and UTSP shall be handled in accordance with the relevant contract between UTSP and the Participant.

1.3.3.8 CA & Repository Licences Trust Marks & Audit:

Certificates are manufactured under this Certificate Policy through the use of a Trustis service which is both accredited to ISO17799 and has attained tScheme approval.

Audit shall be carried out on a periodic basis required to maintain security and trust accreditations. The Auditors that have been approved under this Certificate Policy are:

- Audit resources of contracted Participants providing trust services.
- A certified public accountant with demonstrated expertise in computer security or an accredited computer security professional.

1.3.4 Certificate Manufacturer

The Certificate Manufacturer (Trustis) provides operational Certificate management services for the Issuing Authority. It operates under the terms of the Trustis Service Contract with the Issuing Authority.

The Certificate Manufacturer is approved by the Issuing Authority to manage Certificates on behalf of the Issuing Authority.

The Certificate Manufacturer must demonstrate compliance with this Certificate Policy and any other procedures agreed with the Issuing Authority.

1.3.5 Registration authorities

A PKI may operate with a single or multiple Registration Authorities. Each must demonstrate compliance with this Certificate Policy.

Each Participant is responsible for setting up and operating a Local Registration Authority formed of two or more Enrolment Officers.

UTSP provides an overall Registration Authority that sets up and authorises Local Registration Authorities.

Each Local Registration Authority is responsible for ensuring the eligibility of applicants applying for the Issue of Certificates and check the accuracy and integrity of required information presented by applicants. The Local 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 set out in this Certificate Policy.

Compliance requirements for RAs and LRAs are documented in the Participant Process Definitions supplied by UTSP to the Participants. Such procedures may vary between Registration Authorities. However, in each case they must support the Certification Practice Statement and fully comply with this Certificate Policy.

The following Registration Authorities have been approved by the Issuing Authority to register Subscribers under this Certificate Policy:

- UTSP Issuing Authority.
- UTSP Participant LRA Enrolment Officers.

1.3.6 Certificate Subscribers

A Certificate Subscriber must be a Participant who has signed a UTSP Trust Service Participant Agreement with UTSP or a Participant’s Customer or Participant’s Supplier who has a contract with the Participant that requires them to abide by the obligations set out in the following sections.

1.3.6.1 Eligible Participants

Eligible Participants are

- Those who have met the requirements for joining a Payment Scheme and who have signed or who intend to sign a UTSP Trust Service Participant Agreement with UTSP.
- Those who have signed a UTSP RtP Heads of Terms Agreement.

1.3.6.2 Eligible Certificate Subscribers

Eligible Certificate Subscribers are those Eligible Participants or a Participant Customer or Participant Supplier who has a contract with the Participant that requires them to abide by the obligations set out in the following sections.

1.3.6.3 Obligations of Certificate Subscribers

It is the responsibility of the Certificate Subscriber to:

a) Procure that information submitted by Certificate Subjects in support of an application for a Certificate is true and accurate
b) Ensure Certificate Subscriber holds such rights as necessary to any trade-marks or other such information submitted during the application for a Certificate.
c) Procure that Certificate Subjects diligently review the issued Certificate to confirm the accuracy of the information contained within it before installation and or any use.
d) Provide a trustworthy system for Certificate Subjects to use for the purposes of generating or obtaining a Key Pair and to prevent any loss, disclosure, or unauthorised use of the Private Key
e) Procure that Certificate Subjects keep Private Keys confidential
f) Procure that Certificate Subjects keep confidential any passwords, pass-phrases, PINs or other personal secrets used in obtaining authenticated access to Certificates and PKI facilities
g) Make only true and accurate representations to the Registration Authority and/or Issuing Authority as to the information required to determine eligibility for a Subscriber
h) In accordance with the UTSP Certificate Policy, procure that Certificate Subjects use the Certificate only for legal purposes and restrict it exclusively to those authorised purposes detailed by the UTSP Certificate Policy.
i) Immediately notify the Registration Authority of a suspected or known compromise of Certificate security in accordance with the procedures laid down in the UTSP Certificate Policy.

Certificate Subjects hold Certificates and act on behalf of Certificate Subscribers. The Certificate Subscriber must ensure all responsibilities are met.

For a device or application, the individual responsible for the device or application must accept these responsibilities (see Obligations of Certificate Subjects below).

WARNING: If a Private Key is compromised, unauthorised persons could decrypt or sign messages with the key and commit the Certificate Subscriber to unauthorised obligations.

1.3.7 Certificate Subjects

All Certificate Subjects must be under the jurisdiction and control of a Participant or a Customer or Participant Supplier and must comply with all relevant aspects of this Certificate Policy and other agreements and obligations with the Issuing Authority.

Where a Certificate is Issued for a Certificate Subject that does not directly contract with the Issuing Authority, the Certificate Subscriber will accept the terms and conditions on behalf of the Certificate Subject that is identified in the Certificate. In all cases the Certificate Subscriber is responsible for compliance with the Certificate Policy and all other obligations applicable to it and the Certificate Subject.

The Certificate Subscriber shall bear responsibility for the use of the Private Key associated with the Certificate.

The Certificate Subject Agreement can be found at http://utsp.trustis.com/.

1.3.7.1 Eligible Certificate Subjects

The following types of Certificate Subjects are eligible to be issued with Certificates under this Certificate Policy:

a) Certificate Subjects requiring authenticated access to UK payment or payment related systems of Pay.UK Limited including but not limited to the services the Payment Schemes.
b) Certificate Subjects requiring to digitally sign payment transactions and payment files and other submissions to the Payments Schemes' Central Infrastructure provider(s) by Payment Scheme participants and their authorised customers.
c) The Payments Schemes' Central Infrastructure provider(s) for the purpose of signing files to be sent to Payment Scheme participants.

1.3.7.2 Obligations of Certificate Subjects

It is the responsibility of the Certificate Subject to:

a) Ensure all information submitted in support of an application for a Certificate is true, accurate;
b) Review the issued Certificate to confirm the accuracy of the information contained within it before installation and or any use.
c) Use a trustworthy system for generating or obtaining a Key Pair and to prevent any loss, disclosure, or unauthorised use of the Private Key
d) Keep Private Keys confidential
e) Keep confidential, any passwords, pass-phrases, PINs or other personal secrets used in obtaining authenticated access to Certificates and PKI facilities
f) Make only true and accurate representations to the Registration Authority and/or Issuing Authority as to the information required to determine eligibility for a Certificate Subject
g) In accordance with the UTSP Certificate Policy, use the Certificate only for legal purposes and restrict it exclusively to those authorised purposes detailed by the UTSP Certificate Policy.
h) Immediately notify the Registration Authority of a suspected or known compromise of Certificate security in accordance with the procedures laid down in the UTSP Certificate Policy.

For a device or application, the individual responsible for the device or application must accept these responsibilities.

For Subjects holding Certificates and acting on behalf of Subscribers, the Subscriber must ensure all responsibilities are met.

WARNING: If a Certificate User's Private Key is compromised, unauthorised persons could decrypt or sign messages with the key and commit the Subscriber to unauthorised obligations.

1.3.8 Relying Parties

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

1.3.8.1 Eligible Relying Parties

Relying Parties who are eligible to Rely on Certificates Issued under this Certificate Policy are specified below:

a) Participant (s) of the Trust Service provided by UTSP and their customers.
b) UK payment or payment related systems of Pay.UK Limited including but not limited to the services of the Payment Schemes.
c) The Central Infrastructure provider(s) to the Payment Schemes.

The Relying Party Agreement can be found at http://utsp.trustis.com/ .

1.3.8.2 Relying Parties Obligations

A Relying Party has the following obligations:

a) Relying Parties must comply with the requirements as defined in the Relying Party Agreement at http://utsp.trustis.com/.

b) A Relying Party may justifiably rely upon a Certificate only after:

i. Ensuring that Reliance on Certificates issued under this Certificate Policy is restricted to approved uses only (see Section 1.1.2 (Certificate Use) for a summary of approved usages).
ii. Ensuring, by accessing any and all relevant OCSP Certificate Status Information that the Certificate remains valid and has not been Revoked.
iii. Determining that such Certificate provides adequate assurances for its intended Use.
iv. Take any other precautions prescribed in this Certificate Policy.

1.3.9 Other parties

1.3.9.1 Policy authority

The Policy Authority has ultimate responsibility for governance and control over the Issuance, management and usage of Certificates Issued under this Certificate Policy.

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

The Policy Authority is a part of UTSP.

Contact details:

Policy Authority:
UTSP Policy Authority

Mailing Address:
UTSP Limited,
2, Thomas More Square,
London,
E1W 1YN,
UK
email: UTSP@wearepay.uk

1.3.9.2 Repository

The following Repositories have been approved by the Issuing Authority under this Certificate Policy:

- Entrust (Europe) Limited
- UTSP Limited

Trustis holds data in support of PKI operations. This includes policy and related documentation, Certificates and Certificate Status information.

The Repository provides a community-wide accessible mechanism by which primarily Subscribers and Relying Parties can obtain and validate information on Certificates Issued under this Certificate Policy.

1.4 Certificate usage

Certificate usage is defined by the Certificate Profile. Certificate Profiles must be approved by the Issuing Authority.

1.4.1 Appropriate certificate uses

The categories of transactions, applications, or purposes for which Certificates Issued under this policy may be used are defined in Section 1.1.2 of this Certificate Policy
.

1.4.2 Prohibited certificate uses

All other application use and any other usage categories for Certificates Issued under this Certificate Policy are prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

The Policy Authority is defined in section 1.3.9.1.

Trustis Limited is authorised by the Policy Authority to administer this Certificate Policy. Trustis Limited may be contacted as follows:

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

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

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

1.5.2 Contact person

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

Contact details are provided in Section 1.3.3 of this Certificate Policy.

1.5.3 Person determining CPS suitability for the policy

The Policy Authority (supported by Trustis) determines the suitability of any Certification Practice Statement operating under this Certificate Policy.

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

Contact details are provided in Section 1.3.9.1 of this Certificate Policy.

1.5.4 CPS approval procedures

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

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

An information Repository shall be made available under the terms of this Certificate Policy. The Issuing Authority is the entity with overall responsibility for the operation of a Repository which it may delegate to parties providing Trust Services (please also refer Section 1.3.9.2 of this Certificate Policy).

2.2 Publication of certification information

The following items are published by the Issuing Authority for all parties participating in this PKI:

- This Certificate Policy with its associated PKI Disclosure Statement.
- Any supporting policy documents and agreements.
- The Information that will allow the authenticity of the Certificate of the Issuing Authority to be verified.
- All Certificates of Certificate Authorities Issued by the Issuing Authority (including those for sub-ordinate and superior Certificate Authorities).
- Certificate Status Information for Certificates Issued under this Certificate Policy.

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

2.3 Time or frequency of publication

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

2.4 Access controls on repositories

The Repository (Trustis) must make available the information specified above. However, the Repository may control access to information and restrict such access only to those Trust Service Participants and Relying Parties with specific need for the information.

The Repository shall not prevent access by Participants where required by this Certificate Policy.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Each Subject must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the Certificate subject Name field of Certificates Issued under this Certificate Policy and in accordance with IETF PKIX RFC 5280, updated by RFC 6818. Each Entity may in addition, use an alternative name via the Subject Alternative Name field, which must also be in accordance with IETF PKIX RFC 5280, updated by RFC 6818.

3.1.2 Need for names to be meaningful

The contents of each Certificate Subject name field must have an association with the authenticated name of the Subject. This association may be direct, or where the natural identity of a Subject is required to be hidden, may be recorded elsewhere by the Registration Authority. The Relative Distinguished Name (RDN) may also identify an organisational position or role or link to a Subscriber (if different from the Subject) provided that a person responsible for the oversight of that role is recorded.

A Certificate Issued for a device or application must include within the DN the name of the person or organisation acting as Subscriber for that device or application.

3.1.3 Anonymity or pseudonymity of subscribers

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

3.1.4 Rules for interpreting various name forms

The inclusion of Common Name in a Distinguished Name is mandatory. All other fields that may be included are optional. Their interpretation for any entity shall be as follows:

Element	Description
Common Name	Where the Subject is a natural person, common name may consist of a pseudonym established to hide the natural identity of the Subject. In this case, the fact that the common name is a pseudonym must be made obvious, either by the style of the pseudonym or by explicit indication in common name. Where this hiding is not required, common name shall consist of the given name, middle name or middle initial (if the Subject has a middle name), and the family name of the Subject, in that order, separated by space characters. Where the Subject is a device or application, common name shall consist of sufficient information to uniquely identify the Subject. These name forms may be followed by any other optional information required for identification or for uniqueness of RDN.
Street address	The physical location where the Subscriber resides or conducts business or where the entity can receive paper mail.
Locality name	The city or town or other recognised locality where the Subscriber resides or conducts business.
Country name	The country where the Subscriber resides or conducts business.
Organization name	An organisation with which the Subscriber has a significant relationship. The organization name serves only as an additional identifier of the Subscriber and does not imply employment or any authority to act on behalf of the organisation unless the Certificate and/or its policy specifically provide otherwise.
Subject Alternative Name	Specified only in accordance with IETF PKIX RFC 5280, updated by RFC 6818. Where this specifies an email address, it is the electronic mail address at which the entity can receive electronic mail via the Internet.

3.1.5 Uniqueness of names

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

3.1.6 Recognition, authentication, and role of trademarks

Neither the Policy Authority nor the Issuing Authority is liable for the inclusion of trademarks, trade names or other information under restricted use. Subscriber Agreements shall require

Subscribers to warrant legitimacy of their registration details provided to the Issuing Authority as part of the Registration Process.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

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

3.2.2 Authentication of organisation identity

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

Authentication processes may include face-to-face authentication with a representative of the organisation, or other form of direct registration by representative of the organisation. Where this is the case, the identity of the representative must be authenticated and their authority to represent the organisation must be validated.

Organisational identity may be authenticated via remote means such as public registration provided that the criterion of substantial assurance is satisfied.

Specific requirements for authentication of organisation identity are provided in UTSP's New Participant Take-on Process which is available on request from the Issuing Authority. The Registration Authority shall define and document the mechanisms used to support the level of authentication assurance.

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

3.2.3 Authentication of individual identity

The authentication of Enrolment Officers (Registration Authority Administrators) is set out in UTSP's "Add or Replace Enrolment Officer" process definition which is available on request from the Issuing Authority. This includes the Issuing Authority undertaking face-to-face authentication of one or more initial Enrolment Officers. An authenticated and nominated Enrolment Officer may undertake face-to-face authentication of subsequent Enrolment Officers.

Authentication processes for Certificate applicants may include face-to-face authentication, but not require it. Individual identity may be authenticated by remote means, provided that the criterion of substantial assurance is satisfied.

For PSW contacts, additional requirements for authentication of individual identity are provided in UTSP' "New PSW Contact Registration" process. The Registration Authority shall define and document the mechanisms used to support the level of authentication assurance.

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

3.2.4 Non-verified subscriber information

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

Where non-verified information is incorporated in a Certificate these sources of information are detailed in the UTSP' "New PSW Contact Registration" process and approved by the Issuing Authority.

3.2.5 Validation of authority

Validation of authority (i.e. the determination of whether a Certificate Subscriber has specific rights, entitlements, or permissions, including the permission to act on behalf of an organisation to obtain a Certificate) is the responsibility of the Registration Authorities. Details of validation procedures may be published to Participants.

3.2.6 Criteria for interoperation

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

Requests for interoperation must be directed in the first instance to the Issuing Authority, whose contact details are given in Section 1.3.3 of this Certificate Policy**.**

It is noted that the Bacs Trust Service Code of Conduct does not permit inter-operation of CAs. Hence any such request is unlikely to be granted.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Re-key of Certificates governed by this Certificate Policy is permitted. See also section 4.7 below.

Re-key requests from Subscribers and any participant shall at minimum, incorporate mechanisms for Authentication that fulfil initial authentication requirements. Proof of possession of a valid Certificate as Authentication is permitted.

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.

3.4 Identification and authentication for revocation request

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

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificate applications may be made by:

- A Certificate Subscriber.

- A Certificate Subject acting on behalf of a Certificate Subscriber.
- A representative of a Certificate Subscriber acting on behalf of the Certificate Subscriber.
- A Registration Authority (including Enrolment Officers).

Certificate applicants must comply with the procedures described in this document. Eligible Certificate Subscribers are specified in Section 1.3.6.1 of this Certificate Policy.

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

4.1.2 Enrolment process and responsibilities

A range of enrolment processes are permitted.

The Issuing Authority approves the specific processes associated with a particular enrolment mechanism.

In all cases enrolment processes shall include:-

- Provision of accurate information in support of authentication (and validation of a Certificate Subject or representative of an organisation if applicable).
- Proof of possession of the Private Key.
- Acceptance of the Certificate Subscriber Agreement by the Certificate Subscriber.
- Compliance with this Certificate Policy, obligations of Certificate Subscribers as defined in Section 1.3.6.3 of this Certificate Policy.

4.1.2.1 Registration Authorities and their Representatives

UTSP operates the overall Registration Authority and authorises Participants as part of the setup process following signature of the UTSP Trust Service Participant Agreement with Participant or UTSP RtP Heads of Terms Agreement.

Enrolment of the Participant’s LRA and the Enrolment Officers are approved by the Issuing Authority.

Issuance of Certificates to Enrolment Officers shall be approved by the Issuing Authority or by specifically nominated representatives of the Registration Authority. See Section 3.2.3 above.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

4.2.2 Approval or rejection of certificate applications

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

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

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

Where a Certificate application is rejected, the reasons for rejection may be given to the prospective applicant in accordance with the Issuing Authority “Registration Policy and Procedures”.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA actions during Certificate Issuance

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

4.3.2 Notification to subscriber by the CA of Issuance of Certificate

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

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

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

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

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

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

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

The Certificate Subscriber (or its authorised representative) must acknowledge that it agrees to the terms and conditions stipulated in the Certificate Policy and associated Certificate Subscriber Agreement and any other applicable contractual commitments prior to first use of the Certificate.

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

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

- No unauthorised person has ever had access to the Certificate Subscriber’s Private Key.
- All information given by the Certificate Subscriber to the Issuing Authority or Registration Authority is true and accurate.

The above stipulations may be integrated with the Certificate application process and any smart card or token delivery process as appropriate.

4.4.2 Publication of the certificate by the CA

Publication of the Certificate is permitted. Details of approved Repositories are provided in Section 1.3.9.2 .

4.4.3 Notification of certificate issuance by the CA to other entities

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

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

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Certificate Subscribers must ensure that use of the Private Key associated with the Certificate is consistent with the usage restrictions in the Certificate as stipulated and published by the Issuing Authority. See section 1.1.2.

4.5.2 Relying party public key and certificate usage

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

Relying Parties must satisfy the requirements for reliance on a Certificate defined in Section 1.3.8.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

This Certificate Policy does not support Renewal of Subscriber Certificates.

4.6.2 Who may request renewal

See Section 4.6.1.

4.6.3 Processing certificate renewal requests

See Section 4.6.1.

4.6.4 Notification of new certificate issuance to subscriber

See Section 4.6.1.

4.6.5 Conduct constituting acceptance of a renewal certificate

See Section 4.6.1.

4.6.6 Publication of the renewal certificate by the CA

See Section 4.6.1.

4.6.7 Notification of certificate issuance by the CA to other entities

See Section 4.6.1.

4.7 Certificate Re-Key

4.7.1 Circumstance for certificate Re-Key

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

4.7.2 Who may request certification of a new public key

Re-Key requests may be made by:

- A Certificate Subscriber holding the Certificate.

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

4.7.3 Processing certificate Re-Keying requests

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

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

4.7.4 Notification of new certificate issuance to subscriber

As specified in Section 4.3.2 above.

4.7.5 Conduct constituting acceptance of a Re-Keyed Certificate

Acceptance of a Re-Keyed Certificate is the same as that for Issued Certificates. See Section4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As specified in Section 4.4.2above.

4.7.7 Notification of certificate issuance by the CA to other entities

As specified in Section 4.4.3above.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

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

4.8.2 Who may request certificate modification

See Section 4.8.1.

4.8.3 Processing certificate modification requests

See Section 4.8.1.

4.8.4 Notification of new certificate issuance to subscriber

See Section 4.8.1.

4.8.5 Conduct constituting acceptance of modified certificate

See Section 4.8.1.

4.8.6 Publication of the modified certificate by the CA

See Section 4.8.1.

4.8.7 Notification of certificate issuance by the CA to other entities

See Section 4.8.1.

4.9 Certificate revocation and suspension

Certificate Status Information services shall identify all Revoked and/or Suspended Certificates; at least until their assigned validity period expires.

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

4.9.1 Circumstances for revocation

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

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

A Certificate must be Revoked:

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

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

4.9.2 Who can request revocation

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

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

Approval of a Revocation request may only be granted by:

- The Policy Authority.
- The Issuing Authority.
- An Approved Registration Authority.
- Authorised Registration Authority Operators.

4.9.3 Procedure for revocation request

Revocation must be requested promptly after detection of a compromise or any other event giving cause for Revocation.

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

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

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

- Conduct authentication of the requestor.
- Validate the reason for the request.

- Ensure sufficient information to uniquely identify the Certificate which is the subject of the request.

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

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

4.9.4 Revocation request grace period

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

4.9.5 Time within which RA must process the revocation request

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

- The time for the Certificate Revocation request to be validated, approved and action taken by the Registration Authority. This time is not constrained but the Registration Authority must take all reasonable steps to conduct the Revocation procedure expeditiously.
- The time taken for the Certificate Manufacturer to respond to the authorised Certificate Revocation request. The Certificate Manufacturer must respond promptly to authorised Revocation requests. The maximum time taken for this element is determined by the Issuing Authority in its contract with the Certificate Manufacturer.

4.9.6 Revocation checking requirement for relying parties

A Relying Party may use the mechanisms defined in Section 1.3.8.2 (b) of this Certificate Policy in order to check the Certificate Status Information of the Certificate upon which they wish to Rely and must further verify via a Certificate Revocation List or equivalent on-line protocol that permits authenticity and integrity of the Certificate Status Information.

4.9.7 CRL issuance frequency (if applicable)

The frequency of CRL Issuance is defined in Section 1.1.2 of this Certificate Policy.

4.9.8 Maximum latency for CRLs (if applicable)

The maximum latency of CRL Issuance shall be defined in the contract between the Issuing Authority and the Certificate Manufacturer and published by the Issuing Authority.

4.9.9 On-line revocation/status checking availability

The availability of on-line Certificate Status checking is published by the Issuing Authority in Section 1.1.2.2 of this Certificate Policy.

4.9.10 On-line revocation checking requirements

The requirements on Relying Parties to perform on-line Certificate Status checking are defined in Section 1.3.8.2 of this Certificate Policy.

4.9.11 Other forms of revocation advertisements available

The availability of other forms of Revocation advertisement is published by the Issuing Authority in Section 1.1.2.2 of this Certificate Policy.

4.9.12 Special requirements re key compromise

In the event of the compromise, or suspected compromise, of any Entity's Private Key, an Entity must notify the Issuing Authority or Registration Authority immediately and must indicate the nature and circumstances of the compromise, to the fullest extent known.

4.9.13 Circumstances for suspension

This Certificate Policy does not support Suspension of Subscriber Certificates.

4.9.14 Who can request suspension

See Section 4.9.13.

4.9.15 Procedure for suspension request

See Section 4.9.13.

4.9.16 Limits on suspension period

See Section 4.9.13.

4.10 Certificate status services

4.10.1 Operational characteristics

The types of Certificate Status checking services made available to the Subscriber by the Repository are defined in Section 1.1.2.2 of this Certificate Policy.

4.10.2 Service availability

The availability of any Certificate Status checking services that are available to Relying Parties is, if applicable, are published in Section 1.1.2.2of this Certificate Policy.

4.10.3 Optional features

The optional features of any Certificate Status checking services that are available to the Relying Parties, if applicable, are published in Section 1.1.2.2 of this Certificate Policy.

4.11 End of subscription

- Certificate Subscribers - at the end of a commercial arrangement or subscription, the relevant Certificates may either be Revoked or permitted to expire. The decision on which action to take is made by the Issuing Authority and implemented by the Registration Authority on a case by case basis and is communicated directly to the Certificate Subscriber concerned.

- Service Termination - the actions to be taken in the event of the termination of the service will be defined in the contract between the Issuing Authority, the Certificate Manufacturer and any other Participants providing the Service.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Participants providing trust services shall not offer or support any form of key escrow.

Certificate Subscribers may not facilitate key escrow or recovery mechanisms locally.

Private Key backup policy is defined in Section 6.2.4 below.

4.12.2 Session key encapsulation and recovery policy and practices

This Certificate Policy does not prescribe or control session key management for applications. Use of session key management is a matter for Subscribers.

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

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Where “no stipulation” is stated in this section of the Certificate Policy it indicates there are not specific prescribed requirements for the controls, configuration or security requirements. Where not stipulated, specific details on controls operated for components of the PKI infrastructure must be detailed in the Certification Practice Statement and/or supporting documentation.

Controls must be approved by the Issuing Authority.

5.1 Physical controls

5.1.1 Site location and construction

Sites where Certificate manufacture or time-stamping operations are carried out must:

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

Under this Certificate Policy, the detailed functionality of a Registration Authority may vary. In some scenarios, the Registration Authority is simply a data gatherer that assists the Issuing Authority in gathering Registration or Revocation information from applicants, authenticating applicants, and forwarding the results to the Issuing Authority and/or Certificate Manufacturer. In other scenarios the Registration Authority may additionally initialise and load Certificates and Private Keys into protected stores or tokens. The physical security controls for the various types of Registration Authority will be different.

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

- Registration Authority sites must be located in areas that at least satisfy the controls required for the assurance levels for the level of registration and vetting conducted, and at a minimum be compliant with ISO 27001.

- If a Registration Authority is permitted to submit on-line requests for Certificate Issuance, the Issuing Authority will ensure the operation of the Registration Authority site provides appropriate security protection of the cryptographic module and the Registration Authority Administrator’s Private Key.

- A security container shall be utilised for storing all security devices and tokens used to gain access to the Registration Authority workstation.

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

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

- Ensure unescorted access to the Repository server is limited to authorised personnel.
- Ensure unauthorised personnel are properly escorted and supervised

- Ensure a site access log is maintained and inspected periodically.

Where PINs, pass-phrases or passwords are recorded, they must be stored in a security container accessible only to authorised personnel.

5.1.2 Physical access

See Section 5.1.1 above

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

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

5.1.7 Waste disposal

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

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

5.1.8 Off-site backup

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

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

5.2 Procedural controls

5.2.1 Trusted roles

A Participant providing Trust Services must ensure a separation of duties for critical functions to prevent a single person from maliciously using CA systems and supporting systems without detection.

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

Registration Authorities must ensure that all Registration Authority personnel are adequately trained and understand their responsibility for the identification and authentication of prospective Subscribers and related Certificate management tasks. Registration Authorities shall document arrangements for trusted roles in the Registration Policy and Procedures and/or supporting documentation. Arrangements must be approved by the Issuing Authority or Auditors acting on its behalf.

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

5.2.2 Number of persons required per task

Multi-person control is required for CA Key generation.

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

All other duties associated with Certificate Manufacture or Participants providing other Trust Services may be performed by an individual operating alone, however, verification processes employed must provide for oversight of all activities performed by trusted role holders.

5.2.3 Identification and authentication for each role

All Participants providing Trust Services shall ensure personnel in trusted roles have their identity and authorisation verified before they are:

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

Credentials issued to personnel in trusted roles must be:

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

5.2.4 Roles requiring separation of duties

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

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

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

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

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

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

5.3.2 Background check procedures

See Section 5.3.1 above

5.3.3 Training requirements

See Section 5.3.1 above

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

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

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

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

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

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

- Any log on/off attempts by RA operators.
- All messages from authorised sources requesting an action of the RA and the subsequent actions taken by the RA in response to such requests.
- All messages to the CA requesting an action of the CA and the subsequent action taken by the CA.
- All physical accesses to RA systems (including components) and RA locations.
- RA application start-up and shut down.
- All use of the RA signing key(s).
- Any suspected or known violations of physical security.
- Any suspected or known violations of network and system security.
- All checks made for the registration of RA staff.
- All personnel/role changes for trusted roles.

5.4.2 Frequency of processing log

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

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

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log+

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

5.4.5 Audit log backup procedures

Audit logs and audit summaries must be backed up or if in manual form, must be copied.
Such backups must be provided with the same level of security as the originals and must be commensurate with the data contained within them.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

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

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

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

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

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

Multiple copies of information may be archived.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

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

Records of individual transactions may be released upon request by any of the Participants involved in the transaction, or their recognised representatives.

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

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

5.6 Key changeover

A Certificate Subject may only renew or replace their Certificate and key pair prior to the expiration of the keys, provided that the current Certificate remains valid and has not been Revoked or Suspended. This key changeover may be initiated by one of the following:

- The Certificate Subscriber / Certificate Subject.
- The Registration Authority.
- The Issuing Authority.

Automated notification of an impending required key changeover is permitted.

Certificate Subjects without valid keys must be re-authenticated in the same manner as for an initial registration.

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

All Issuing Authority signing keys shall be generated and a new Certificate corresponding to these keys shall be Issued at least three months prior to the expiration of the old Certificate.

After generation of the new Issuing Authority CA signing keys, the Issuing Authority shall cross certify according to the requirements for cross certification as approved by the Policy Management Authority and must include the following:

- The Issuing Authority holding the new private CA-key shall Issue one Certificate for the old public CA-certificate signed with the new private CA-key.
- The Issuing Authority holding the old private CA-key shall Issue one Certificate for the new public CA-certificate signed with the old private CA-key.

All CA-certificates shall be made available in a repository accessible to all Participants in the PKI.

All copies of old Issuing Authority Private Keys shall be:

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

A business continuity plan shall be in place to protect critical Public Key infrastructure processes from the effect of major compromises, failures or disasters. These shall enable the recovery of all Issuing Authority services. Business continuity plans for Participants providing Trust Services shall be detailed in the Certification Practice Statement and/or supporting documentation. Plans must be approved by the Issuing Authority or Auditors acting on its behalf.

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

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

- Disabling the OCSP validation authority thereby causing all relying party certificate status validation requests to fail. See Certificate Policy section 5.7.1.
- Notification to PKI parties of the compromise.
- Revocation of certificates.
- Publication of status information.
- Rebuild of the affected systems and the re-issuance of certificates.
- Other action as necessary, agreed between the Issuing Authority and Participants.

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

5.7.2 Computing resources, software, and/or data are corrupted

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

5.7.3 Entity private key compromise procedures

See Section 5.7.1 above.

5.7.4 Business continuity capabilities after a disaster

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

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

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

5.8 CA or RA termination

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

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

- Inform both the Issuing Authority and Policy Authority for the governing Certificate Policy.
- Provide a notice period of not less than 1 year after the initial term of 5 years.
- Revoke all relevant CA and Subscriber Certificates at the end of 90 days if required by the Issuing Authority.
- Arrange with a third party for the preservation and storage of records for the minimum period of time stipulated for the service being terminated but in any event not less than 7 years.

Registration Authority - Registration Authorities deployment and configuration details vary. At minimum the Registration Authority terminating service shall:

- Have all RA keys under their control Revoked.
- Have all RA Operator, Vettor and Pre-Authorisation manager Certificates Revoked
- Ensure preservation and storage of records for the minimum period of time stipulated for the service being terminated but in any event not less than 7 years. Alternatively with the approval of the Issuing Authority, records may be transferred to another Participant providing Trust Services, e.g. a new or alternative Registration Authority.

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

6 TECHNICAL SECURITY CONTROLS

Where “no stipulation” is stated in this section of the Certificate Policy it indicates there are not specific prescribed requirements for the controls, configuration or security requirements.

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

6.1 Key pair generation and installation

6.1.1 Key pair generation

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

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

Certificate Subjects' Key Pairs may be generated by the Certificate Subject or Registration Authorities approved by the Issuing Authority to conduct key generation. Procedures must be approved by the Issuing Authority or Auditors acting on its behalf.

Keys used for signing shall only be generated by the Certificate Subject or generated under the direct control of the Certificate Subject.

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

6.1.2 Private key delivery to subscriber

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

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

- Controls shall be in place to ensure the Certificate Certificate Subject shall replace initial activation data for the security environment with personally chosen activation data.

6.1.3 Public key delivery to certificate issuer

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

Registration Authority - The mechanism by which Certificate Subscriber' Public Keys are delivered to the Certificate Manufacturer through the Registration Authorities is defined by the Issuing Authority and described in the Issuing Authority "Registration Policy and Procedures".

6.1.4 CA public key delivery to relying parties

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

6.1.5 Key sizes

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

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

6.1.6 Public key parameters generation and quality checking

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

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Certificates Issued under this policy may be used in applications and services as listed in Section1.1.2. A Certificate may be used for one or more of the following key usage services:

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

Where a Certificate has been issued under this policy for the key usage service of non-repudiation the Private Key shall be used solely for the purpose of non-repudiation.

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

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

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

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

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

6.2.2 Private key (n out of m) multi-person control

For any Issuing Authority and supporting CA-Keys and keys that affects the outcome of Issued Certificates and Certificate Status Information services, at a minimum two-person control is required.

6.2.3 Private key escrow

Subscribers (Subjects) may not undertake escrow arrangements for their own Private Keys.

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

6.2.4 Private key backup

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

Certificate Subscribers and Certificate Subjects may backup their own keys.

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

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

6.2.5 Private key archival

No stipulation.

6.2.6 Private key transfer into or from a cryptographic module

If Certificate Subscribers' Private Keys are not generated in the Entity's cryptographic module, it must be entered into the module via the use of a secure procedure approved by the Issuing Authority. Mechanisms to protect key material and any associated activation data from unauthorised access, modification and use shall be employed.

Participants conducting such key transfer shall provide detail of the procedure in a Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or Auditors acting on its behalf. See Section 6.1.2 above.

6.2.7 Private key storage on cryptographic module

For any Issuing Authority and supporting CA-Keys and keys that affects the outcome of Issued Certificates and Certificate Status Information services and other business processes prescribed standards are required for the cryptographic protection of Private Keys. See Section 6.2.1 below.

6.2.8 Method of activating private key

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

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

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

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

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

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

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

Whether active, expired or archived, the Issuing Authority must approve the destruction of Issuing Authority and supporting CA-Keys.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

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

6.3.2 Certificate operational periods and key pair usage periods

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

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

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

6.4 Activation data

6.4.1 Activation data generation and installation

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

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

6.4.2 Activation data protection

All Issuing Authority, supporting CA-Keys and keys that affect the outcome of Issued Certificates and Certificate Status Information services shall have mechanisms for the protection of activation data which is appropriate to the Keys being protected.

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

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Participants providing Trust Services shall implement security measures that have been identified through a threat assessment exercise and must cover the following functionality where appropriate:

- Access control to trust services and PKI roles.
- Enforced separation of duties for PKI roles.
- Identification and authentication of PKI roles and associated identities.
- Use of cryptography for session communication and database security.
- Archival of Participant history and audit data.
- Audit of security related events.
- Trusted path for identification of PKI roles and associated identities.
- Recovery mechanisms for keys of PKI Participants providing trust services.

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

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

6.5.2 Computer security rating

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

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

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

6.6 Life cycle technical controls

6.6.1 System development controls

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

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

6.6.2 Security management controls

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

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

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

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

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

6.8 Time-stamping

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

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

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

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

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

7.1.1 Version number(s)

Only Certificates conformant to X.509 Version 3 and IETF RFC 5280, updated by RFC 6818 may be Issued.

7.1.2 Certificate extensions

All End Entity PKI software must correctly process the extensions identified in sections 4.2.1 and 4.2.2 of the IETF RFC 5280, updated by RFC 6818 Certificate Profile Specification. The following are common Certificate extensions:

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

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

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

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

This Certificate Policy has been assigned an OID as defined in section 1.2.1. This shall be included in the certificate Policies extension of all Certificates Issued under this Certificate Policy.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

Only Certificate Revocation Lists conforming to X.509 version 2 and IETF RFC 5280, updated by RFC 6818 may be issued.

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

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

7.3.1 Version number(s)

OCSP and other forms of Certificate Status Information provision are permitted.

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

Mechanisms for on line Certificate Status discovery shall be specified in Section1.1.2.2.

7.3.2 OCSP extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

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

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

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

For Certificate Manufacturers, audit shall be conducted by an approved third party auditor and conducted not less than annually.

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

8.2 Identity/qualifications of assessor

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

Approved Auditors are as defined in Section 1.3.3.8 of this Certificate Policy and may include internal auditing resources of Participants or a TSP, subject to the approval of the Policy Authority.

For Certificate Manufacturers audit shall be conducted by an approved third party auditor.

8.3 Assessor's relationship to assessed entity

The acceptability of auditors is decided by the Policy Authority.

8.4 Topics covered by assessment

Audit is required to ensure a party providing Trust Services *(also refer to Section 1.3 where it identifies Trust Service Providers)* is operating in accordance with its Certification Practice Statement, this Certificate Policy and any declared assurance or approval schemes under which Trust Services are operated.

Where the Trust Service Providers uses any designated authorised agents in order to provide service, the audit shall include the operations of such designated authorised agents.

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

8.5 Actions taken as a result of deficiency

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

8.6 Communication of results

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

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

9 OTHER BUSINESS AND LEGAL MATTERS

Although RFC 3647 has an extensive list of other business and legal matter headings, these are contractual matters and have been devolved to the contractual arrangements between the parties involved in the Trust Service.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The Issuing Authority shall establish any fees for the Issuance of Certificates. Where fees are charged, the fee schedule shall be published and available to Participants in the UTSP Trust Service Participant Agreement and/or the UTSP RtP Head of Terms Agreement or published/communicated in such other document or form as may be agreed between UTSP and the Participant. .

9.1.2 Certificate access fees

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

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

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

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

9.1.5 Refund policy

The refund policy is set out in Section 1.3.3.6 of this Certificate Policy.

9.2 Confidentiality of business information

9.2.1 Scope of confidential information

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

All private and secret keys and associate activation data, used or otherwise handled Participant operating under this Certificate Policy shall be kept confidential unless required otherwise by law.

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

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

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

9.2.2 Information not within the scope of confidential information

Certificates and Certificate Status Information are not classified as Confidential or as private. Identification information or other personal or corporate information appearing on Certificates is not considered Confidential.

.

9.3 Privacy of personal information

See section 1.3.3.4

9.4 Individual notices and communications with participants

9.4.1 Certificate Subscribers

Whenever any Certificate Subscriber hereto desires or is required to give any notice, demand, or request with respect to this Certificate Policy, such communication shall be made either by using digitally signed messages consistent with the requirements of this Certificate Policy, or by paper-based communications. Electronic communications shall be effective upon the sender receiving a valid, digitally signed acknowledgment of receipt from recipient. Such acknowledgement must be received within five working (5) days, or else notice must then be given by paper-based communications. Such paper-based communications must be delivered by a service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed to the Issuing Authority as detailed in Section 1 1.3.2 of this Certificate Policy. All such communications shall be effective upon receipt.

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

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

9.4.2 Issuing Authority

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

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

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

9.4.3 Notification

Any notices given in 9.11.2 shall be deemed served effective upon dispatch.

9.5 Amendments

9.5.1 Procedure for amendment

Amendments to this Certificate Policy fall into three categories:

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

Where the amendments are likely to have a major impact on the majority of users of this Certificate Policy then it must be replaced by a new document (ref. Section 9.12.3).

9.5.2 Notification mechanism and period

All proposed changes that may materially impact users of this Certificate Policy will be managed in accordance with the Change Control Procedures set out in the Trustis Service Contracts or in the Participant Agreements as relevant.

9.5.3 Circumstances under which OID must be changed

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

9.6 Dispute resolution provisions

All disputes in regards to the Certificate Policy shall be referred in writing to the Issuing Authority. The Issuing Authority shall deal with such disputes in accordance with its dispute resolution process specified in Section 1.3.3.7 of this Certificate Policy.

9.7 Governing law

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

9.8 Compliance with applicable law

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

9.9 Miscellaneous provisions

9.9.1 Certificate Policy Content

Section and paragraph headings shall not affect the interpretation of this Policy.

9.9.2 Third party rights

Save as expressly provided for in this Certificate Policy or a Policy Document, no term of this Policy shall be enforceable under the Contracts (Rights of Third Parties) Act 1999 by a third party. The parties who have such rights are the Participants.