Controlling Document

Telstra (AD) Certificate Chain Certificate Practices Statement

Published By: Telstra PKI Team

Published Date: 30th September 2024

Telstra Corporation Limitd
ABN 33 051 775 556

Telstra Corporation Limited Certificate Practices Statement

Trademark Notices

REVISION HISTORY

Version	Date	Revision Detail	Author	Status
2.1	September 2024	Reviewed	PKI Team	Published
2.0	August 2024	Review & update	PKI Team	Draft
1.0	2010	First publication	PKI Team	Baseline

Table of Contents

1. PURPOSE

In a public key infrastructure (PKI), a certification authority (CA) acts as a trusted party to facilitate the confirmation of the relationship between a public key and a named entity. The CA handles all aspects of the certificate management for a PKI. This document presents the comprehensive requirements of the Telstra CA operation in the Telstra Corporation Limited Telstra) environment, to ensure **Confidentiality**, **Integrity**, **Authenticity** and **Non-repudiation**.

Telstra Certification Practice Statement (CPS) is a statement of the practices that Telstra CA employs in issuing digital certificates and providing digital certificate services. This Telstra PKI CPS applies to the digital certificate infrastructure of Telstra and Telstra Digital Certificate Services and relates only to infrastructure and Digital Certificates used by Telstra internal Subscribers to access Telstra environments and Designated Products.

It is expected that this document will be revisited and revised from time to time to ensure its continued reliability as an operational requirement for CAs. All capitalized terms in this Telstra PKI CPS are defined in a consolidated Glossary document in PKI knowledgebase and the provisions for interpretation and construction, severance, waiver and governing law contained in the Telstra PKI Digital Certificate Terms and Conditions also apply to this Telstra PKI CPS.

Telstra PKI Services has three CPS documents to differentiate its internal first-party (not publicly trusted) (This CPS) from its external first-party (publicly trusted) CA operations (future CPS) and its third-party issued Code signing certificates (Future CPS), as they are regulated by separate compliance authorities and/or levels.

This document does not aim to provide legal advice or recommendations. Telstra MAY publish additional Certificate Policies or Certification Practice Statements, as necessary, to describe other products or service offerings. The Telstra Corporation Limited RCA CPS is published at: telstra-pki.pki.telstra.com.au - /cps/

1.1. Document Identification

The commencement date of the Telstra Root Certification Authority Certification Practice Statement (Issuing CA CPS) is the date the Telstra Issuing CA generates it's self-signed certificate. The commencement date of this CPS is**: 30th Sept 2024**

Telstra PKI has been assigned an X.500 Object Identifier (OID) to Telstra Issuing CA CPS. The authority for issuing an OID is the Telstra PKI Policy Management Authority (Telstra PMA). The Policy Object Identifier Designation for this CPS is registered under the Policy Management Authority. The OID for the Telstra Issuing CA Certificate Practices Statement (Telstra Issuing CA CPS) is **OID =** 1.3.6.1.4.1.1088.4.27.5.2.1 *(need to update to AD CA OID)*

The legacy Telstra PKI Issuing CA has different OID which is descripted in Legacy Telstra PKI Issuing CA CPS.

2. SCOPE

Telstra Issuing CA CPS is a practices statement that the Telstra Issuing CA employs in providing certification services. This CPS sets forth the business, legal and technical practices and procedures for managing digital certificates within the Telstra Trust Environment (TTE), collectively, Telstra Corporation Trust Environment Participants. More specifically, this CPS provides the context under which certificates are requested, created, issued, renewed, and/or used by Subscribers. In accordance with the requirements of the CPS and TTE Standards, the CPS describes the practices that

Telstra employs for:

- Securely managing the core infrastructure that supports the TTE, and
- Managing Certificates throughout the certificate lifecycles within Telstra's subdomain of the TTE, the scope of this document is limited to Telstra internal Issuing CA CPS.

This document is written in accordance with RFC3647 Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework (version 3)**,** and outlines the scope and rules applying to Telstra PKI certificates. This CPS is specifically applicable to:

- Telstra Root CA (AD)
- Telstra Internal Issuing CA *(as differentiated to external first party and third-party Issuing CAs)*

Telstra PKI currently offers the above two classes of CA within its sub domain of the TTE. This CPS describes how Telstra PKI meets the Telstra Certificate Policy (CP) requirements for each class within TTE, including practices and procedures concerning the issuance and management of all certificates by the two CA classes.
Telstra may publish Certificate Policies that are supplemental to this CPS in order comply with the specific policy requirements of government, or other industry standards and requirements. These supplemental certificate policies shall be made available to subscribers for the certificates issued under the supplemental policies and their relying parties.

3. INTRODUCTION

This document content is divided into nine sections:

- Section 3 – provides an overview of the CPS and set of provisions, as well as the types of entities and the appropriate applications for certificates.
- Section 4 – contains any applicable provisions regarding identification of the entity or entities that operate repositories; responsibility of a PKI participant to publish information regarding its practices; certificates; the current status; frequency of publication; and access control on published information.
- Section 5 – covers the identification and authentication requirements for certificate related activity.
- Section 6 – deals with certificate life-cycle management and operational requirements including application for a certificate, revocation, suspension, audit, archival and compromise.
- Section 7 – covers facility, management, and operational controls (physical and procedural security requirements).
- Section 8 – provides the technical controls about cryptographic key requirements.
- Section 9 – defines requirements for certificate, Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) formats. This includes information on profiles, versions, and extensions used.
- Section 10 & 11 – Compliance audit and other business & legal matters are out of scope for this CPS

3.1. Common Elements

This Telstra PKI CPS covers the common practices and procedures that apply to the entire Telstra PKI Hierarchies, as operated by Telstra Corporation Limited under control of the Telstra PKI Policy Management Authority**.** The common elements include:

- Use of evaluated products for any of the security-critical cryptographic operations.
- Separation of registration and certification operations, with registration operations generally being performed on a remote site managed and operated by the Telstra PKI operations.
- Employment of trustworthy personnel who have been independently vetted to manage critical Telstra assets.
- Application of rigorous change control processes to ensure no change is introduced without due consideration of all its possible security impacts, and
- The institution of a continuous cycle of internal review and assessment to ensure a high level of operational integrity is always maintained.

3.2. Overview

A certificate binds a public key held by an entity (such as a device, person, organization, account or website) with set of information that identifies the entity, this entity is known as the "subject" or "subscriber" of the certificate. Two exceptions:

1. Devices (in which the subscriber is usually the individual or organization controlling the device) and
2. Anonymous certificates (in which the identity of the individual or organization is not available from the certificate itself).

A certificate relies upon the accuracy of the binding between the subject public key and the identity contained in that certificate. A relying party is an entity that uses a public key in a certificate (for signature verification and/or encryption). In other words, the relying party is also known as the service provider, since this entity (Telstra internal domain server) that needs to reply on the authentication (via the public key).
The degree to which a relying party can trust the binding embodied in a certificate depends on several factors. For example, CA's authentication practice to the subject; the CA's operating policy, procedures, and security controls; the scope of the subscriber's responsibilities (for example, in protecting the private key); and the stated responsibilities and liability terms and conditions of the CA (for example, warranties, disclaimers of warranties, and limitations of liability). Within this context, A CP (Certificate Policy) is "a named set of rules that indicates the applicability of a certificate to a particular Telstra domain and/or applications with common security requirements."

In the Telstra PKI, the hierarchy of Trusted Elements comprises three level hierarchies of certificates.

1. Root CA;
2. Issuing CA;
3. Leaf certificate.

The CPS is only one of a set of documents relevant to Telstra PKI and digital certificate services. The other documents may include:

- The Telstra Physical Security Standard V8.0 (Feb 2024), which sets forth security principles governing the TTE infrastructure,
- The Telstra Security and Audit Requirements Guide, which describes detailed requirements for Telstra Corporation Limited and Affiliates concerning personnel, physical, telecommunications, logical, and cryptographic key management security, and
- Key Ceremony Reference Guide, which presents detailed key management operational requirements.
- Ancillary agreements imposed by Telstra. These agreements bind Customers,

Subscribers, and Relying Parties of Telstra. Among other things, the agreements flow down TTE Standards to these TTE Participants and, in some cases, state specific practices for how they must meet TTE Standards.

3.2.1. Relationship between the Certificate Practice Statement and Certificate Policies

The CP states the requirements for the issuance and management of certificates issued by Telstra CAs, and requirements for the operation of the CAs. The CPS states how the Telstra CA(s) implement the requirements. Each CA that issues certificates under this CP must have a corresponding approved Telstra CPS.
As Telstra Enterprise PKI is an internal private PKI service, the CP or CPS has no contractual significance these CPs and CPSs to be strictly informational and disclosure documents. Telstra Root Certification Authority Certificate Practice Statement.
This Telstra CPS relates to:

- The authentication and confidentiality Certificates signed by the Telstra Root CA.
- The authentication and confidentiality Certificates signed by the Telstra Root CA and issued to Telstra Subordinate Certification Authorities.

Please refer to Telstra PKI Certificate Policy documents (for each trust chain)

3.3. Obligations

3.3.1. CA Obligations

The Telstra CA is responsible for all aspects of the issuance and management of a certificate, including control over the application and enrolment process, the identification and authentication process, the actual certificate manufacturing process, publication of the certificate, suspension and revocation of the certificate, and renewal of the certificate. Ensuring that all aspects of the Certificate services, operations and infrastructure are performed in accordance with the requirements, representations, and warranties of this CPS.

The Telstra CA operates in accordance with all applicable legislations of the Commonwealth of Australia when fulfilling these obligations. The Telstra CA will take all reasonable measures to ensure that Subscribers and Relying Parties are aware of their respective rights and obligations with respect to the operation and management of any keys, Certificates or End-Entity hardware and software used within the framework established by this CPS.

3.3.2. Repository Obligations

Certificates and CRLs are available to relying parties in accordance section 4.1.

3.3.3. Registration Authorities (RA) Obligations

The Telstra CA shall be responsible for performing all identification and authentication functions and all certificate manufacturing and issuing functions. However, Telstra CA may delegate these functions to an identified registration authority (RA), i.e. Dcerts, provided that the Telstra CA remains primarily responsible for the performance of those services in a manner consistent with the requirements of this CPS.

3.3.4. Subscriber Obligations

In some cases, the Telstra CA may require the subscriber (”certificate applicant”,

used interchangeably in this document) to enter into an agreement for the benefit of relying parties obligating the subscriber to:

- Ensure any information required to be submitted to a CA or RA in connection with a certificate must be complete and accurate.
- Activate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure, or unauthorised use of the private key.
- Acknowledge that by accepting the certificate the subscriber is warranting that all information and representations made by the subscriber that are included in the certificate are true.
- Use the certificate exclusively for authorised and legal purposes, consistent with the corresponding certificate policy and CPS.
- Request the Telstra (issuing) CA to revoke the certificate promptly upon any actual or suspected compromise of the subscribers private key.

3.3.5. Relying Party Obligations

A relying party has a right to rely on a certificate that references this CPS only if the certificate is used and relied upon for lawful purposes and under circumstances where:

- The reliance was reasonable and in good faith in light of all the circumstances known to the relying party at the time of reliance.
- The certificate is used for an appropriate purpose according to this CPS.
- The relying party checked the status of the certificate prior to reliance and it was valid.

3.3.6. PKI Policy Management Authority (PMA) Obligations

The PMA is responsible for the terms of this CPS and its administration.

3.4. Representations by Telstra CA

By issuing a certificate that references this CPS, the Telstra CA certifies to the subscriber, and to all relying parties who reasonably and in good faith rely on the information contained in the certificate during its operational period that:

- The Telstra CA has issued, and will manage, the certificate in accordance with this CPS, any applicable PMA regulations and any applicable state statute or regulations and that the certificate meets all material requirements of this CPS.
- Operate in accordance with this CPS, and applicable laws of the Commonwealth of Australia when issuing and managing the keys provided to RAs and Subscribers under this CPS.
- Ensure that all CAs, RAs, repositories and certificate manufacturing authorities operating on its behalf are aware of, and agree to abide by, the stipulations in this CPS that apply to them.
- Have in place mechanisms and procedures approved by the PMA to ensure that subscribers and relying parties (collectively known as End-Entities) are aware of, and agree to abide by, the stipulations in this CPS that apply to them and their respective rights, obligations and liabilities. if any, with respect to the operation and management of any keys, certificates or End-Entity hardware and software connected with Telstra PKI.
- There are no misrepresentations of fact in the certificate known to the Telstra CA, and the Telstra CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS.
- Information provided by the subscriber in the certificate application for inclusion

in the certificate has been accurately transcribed to the certificate.

3.4.1. Notification of certificate issuance and revocation

Telstra CAs will make CRLs available to subscriber's or relying parties in accordance with this CPS, Telstra Issuing CA's will notify a subscriber when a certificate bearing the subscriber's DN is issued, suspended, reinstated, or revoked.

3.4.2. Accuracy of representations

Telstra CA publishes and certifies a certificate, when an issuing CA publishes certificate to a subscriber it certifies a certificate that it has issued. The information stated in the certificate was verified in accordance with this CPS. Publication of the certificate in a repository, to which the subscriber has access, constitutes notice of such verification. The Telstra CA will provide to each subscriber notice of the subscriber's rights, obligations and liabilities, if any, under this CPS. Such notice will be in the form of an agreement, as specified by the PMA, that includes, but not be limited to,

- A description of the allowed uses of certificates issued under this CPS.
- The subscriber's obligations concerning key protection; and procedures for communication between the subscriber and the Telstra issuing CA or RA, including communication of changes in service delivery or changes to this CPS.
- Subscribers will also be notified as to procedures for dealing with suspected key compromise, certificate or key renewal, service cancellation, and dispute resolution.

The Telstra CA ensures that any notice of the subscriber's rights, obligations and liabilities, if any, under this document includes a description of a relying party's obligations with respect to use, verification and validation of certificates.

3.4.3. Time Between certificate request and issuance.

There is no general stipulation for the period between the receipt of an application for a Certificate and the generation of the entity's key material.

3.4.4. Certificate revocation and Renewal

Telstra CA must ensure that any procedures for the expiration, revocation and renewal of a certificate will conform to the relevant provisions of this CPS and will be expressly stated in any other applicable document outlining the terms and conditions of the certificate use. The CA must ensure that the key changeover procedures are in accordance with 6.3 and 6.4. The CA will also ensure that notice of revocation of a certificate will be posted to the CRL within the time limits stated in 6.2.9.2. The address of the CRL is defined in the certificate.

3.4.4.1. Revocation Request

Telstra CA, or RA acting on its behalf, must authenticate a request for revocation of a certificate. The Telstra CA must establish and make publicly available the process by which it addresses such requests and the means by which it will establish the validity of the request in accordance with 6.2.9. All Requests for revocation of certificates will be logged.

3.4.4.2. Circumstances for revocation

A subscriber may request revocation of their individual certificate at any time for any reason. The CA may also revoke a certificate upon failure of the subscriber to meet its obligations under this CPS, or any other agreement, regulation, or legislation applicable to the certificate that may be in force. This includes revoking a certificate when a suspected or known compromise of the private key has occurred.

3.4.4.3. A certificate must be revoked

- When any of the information in the certificate changes (a new certificate issued as replacement).
- Upon suspected or known compromise of the private key.
- Upon suspected or known compromise of the media holding the private key.

3.4.4.4. Who can request revocation

The revocation of a certificate may only be requested by:

- The subscriber in whose name the certificate was issued.
- The individual or organizational unit that made the application for the certificate on behalf of device or application.
- Personnel of the Issuing CA if the CA determines that the certificate was not properly issued in accordance with this policy and/or any applicable CPS.

3.4.4.5. Procedure for revocation request

The Telstra CA will ensure that all procedures and requirements with respect to the revocation of a certificate are set out in the CPS, or otherwise made publicly available. An authenticated revocation request, and any resulting actions taken by the Telstra Issuing CA, will be recorded and retained. In the case where a certificate is revoked, full justification for the revocation must also be documented. Where an Entity certificate is revoked, the revocation will be published in the appropriate CRL.

Any action taken as a result of a request for the revocation of a certificate must be initiated immediately if the request is received during local business hours of the Telstra Issuing CA.

3.4.4.6. Circumstances for Certificate suspension (or hold)

If the Telstra Issuing CA or RA receives notification from a subscriber that there is cause to revoke a certificate using the criteria stated in 3.2.11.1 but the authenticity of the request cannot be immediately verified by the Telstra Issuing CA or RA, the Telstra Issuing CA or RA may initiate a certificate suspension. A revocation request that is submitted electronically with a digital signature based on the old key pair is subject to prompt revocation once authenticated based on that key pair.

3.4.4.7. Who can request Suspension

The Telstra Issuing CA or RA may initiate a certificate suspension.

3.4.4.8. Procedure for suspension request

The Telstra Issuing CA must either revoke or reinstate the suspended certificate during the suspension period and publish the status changes resulting from the suspension and its subsequent revocation or reinstatement.

3.4.4.9. Protection of private keys

All Entities must ensure that their private keys and activation data are protected in accordance with section 3.3 herein.

3.4.4.10. Restrictions on issuing CA's private keys

An Issuing CA must ensure that its certificate signing private key is used only to sign certificates and CRLs. Such CA may issue certificates to Subscribers, CA and RA personnel, devices and applications. An Issuing CA will ensure that private keys issued to its personnel to access and operate CA applications are used only for such purposes. If required, its personnel could be issued sets of Subscriber keys and certificates to be used for purposes other than CA use.

3.5. Private Key Protection and Cryptographic Module Engineering Controls

The certificate holder must protect its private keys from disclosure. Please refer to Section 8 for details.

4. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The Telstra Issuing CA will:

- include within any certificate it issues the URL of a web site maintained by, or on behalf of, the CA, server.
- ensure the publication of this CPS, on a web site maintained by, or on behalf, of the Telstra Issuing CA.
- ensure, directly or through agreement with a repository, that operating system and repository access controls will be configured so that only authorised CA personnel can write or modify the online version of this CPS.
- provide a full text version of its CPS when necessary for the purposes of any audit, inspection, accreditation or cross-certification.
- All information to be published in the Repository shall be published promptly after such information is available to the Telstra Issuing CA.

4.1. Repositories

The Telstra CA will have two repositories that hold both certificates and CRLs. The CRL repository should be publicly available in order to allow relying parties access to CRL data. Where the certificate repository is operated in a different computing environment other than the CA, the certificate and CRL content shall remain under control of Telstra PKI.

The Telstra CA:

- May make available, to relying parties, a certificate repository of issued certificates.
- Shall make available, to relying parties, certificate revocation information (CRLs and/or OCSP, published by the Telstra Issuing CA in accordance with the requirements of Section 4.9 and 4.10
- Shall make available a copy of this CPS for subscriber (and/or certificate applicant) and relying party review.
- The repository for all PKI certificates issued under this Telstra Issuing CA CPS is the Account-01 Active Directory.
- The Account-01 active directory provides information about active certificates, revoked certificates and expired certificates.
- Certificate revocation status is published at this internet facing web server http://telstra-crl.pki.telstra.com.au/
- This CPS is available at an internet facing web server http://telstra-crl.pki.telstra.com.au/
- Changes in the status of certificates issued under this Telstra CA CPS, including revocation and expiry of certificates will be published in the Account-01 active directory by the Telstra Issuing CA. *(CRLs are stored in Active Directory under 'CN=CDP, CN=Public Key Services, CN=Services, {ConfigurationNamingContext}'. A subcontainer is created for each CA under CDP container.)*

The Telstra Corporation Limited Account-01 active directory:

- does not publish reasons why a certificate has been revoked.
- only publishes information already contained in the certificate, and
- The Telstra Account-01 active eirectory is accessible programmatically.
- The Telstra Account-01 active directory is available 7 days a week, 24 hours a day.

4.2. Publication of Certificate Information

Subscribers shall be notified that the Telstra CA may publish information submitted by them to publicly accessible directories in association with certificate status information. Certificate and CRL publication shall be in accordance with Section 6.2.

The Telstra CA reserves the right to make available and publish information on its policies and practices by any means it sees fit. Due to their sensitivity, Telstra CA may refrain from making publicly available certain subcomponents and elements of such documents including certain security controls, procedures related with the CA functioning, etc.

The Telstra CA shall provide full text version of this CPS when necessary for the purposes of audit, accreditation or as required by law.

4.2.1. Publication of Telstra Issuing CA Information

Certificates and their corresponding hash values are published to the Account-01 active directory when the certificate is generated. In addition, the hash value of the Telstra Issuing CA and Telstra CA certificate is published on Telstra website, http://telstra-pki.pki.telstra.com.au/cps/

Publication of Policy and Practice Information

This Telstra CA CPS is published electronically at the website, http://telstra-pki.pki.telstra.com.au/cps/

Formal notification of changes to this Telstra Issuing CA CPS will not be given to any entities. Notification of changes will be provided on Telstra website http://telstra-pki.pki.telstra.com.au/cps/ . Interested parties must exercise due care and check, on a regular basis, the Telstra website to review and monitor any changes in the Telstra CA CPS. Interested parties are responsible for retrieving amendments when a revised and/or amended Telstra CA CPS is posted to the website.

4.3. Frequency of Publication

Certificate information shall be distributed and/or published promptly upon issuance. Maximum time limits and frequency of certificate and CRL publishing are described in section 6 of this CPS. Updates to this CPS are published in accordance with PKI operational policies. Other relevant PKI documentations are published as necessary.

4.3.1. Frequency of publication of this CPS

Properly documented CPS keeps the PKI assets trusted over the time and serves as a basis for integrated processes and procedures. The combination of the CPS and its corresponding CP is continuously updated and changed as technologies, security, and compliance requirements change. New and revised approved versions of this Telstra Issuing CA CPS are published promptly at, http://telstra-pki.pki.telstra.com.au/cps/.

4.4. Access Control

The Telstra CA keeps access to its public repository available to relying parties with the purpose of validating certificates the CAs have issued and access to this CPS. The Telstra CA may limit or restrict access to its services such as the publication of status information on external databases and private directories. Access controls may be instituted at the discretion of the Telstra CA.

5. IDENTIFICATION AND AUTHENTICATION

This section sets out the process that applicants go through to authenticate themselves and register for Telstra PKI Certificates and binding key pairs. The certificate request must be submitted by an individual either on their own behalf or on the behalf of the device or application server that will use the certificate. In the cases where the certificate applicant will not be the certificate-owner, it also describes the requirements for establishing that the certificate applicant is authorised to submit the request on behalf of the eventual certificate-owner. Alternately, the request can be submitted by an agent or agent process authorised by the Telstra CA, to request certificates on the behalf of the subscriber. However, in these cases, the agent must assure the identity of the subscriber through authentication of that user's or system's credentials. The user's or system's credentials must be bound uniquely to only the person or system represented by those credentials. The events requiring proof of identity are as follows:

- Initial registration,
- Revocation requests.

5.1. Naming

5.1.1. Initial Registration

Each Entity must have unique name.

5.1.2. Types of Names

Each Entity must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate Subject Name field and in accordance with PKIX Part 1.

Detailed naming standard and mechanism is discussed in a separate Telstra PKI Identification and Authentication Policy.

5.2. AUTHENTICATION

5.2.1. Recognition authentication and roles of trademarks

This section is out of scope for the current Telstra PKI Issuing CA.

5.2.2. Method to prove possession of private key

The method to prove possession of a private key shall be PKCS #10 - Certificate Signing Request (CSR), or another cryptographically equivalent request (digitally signed request with private key). Detailed naming standard and mechanism is discussed in a separate Telstra PKI Identification and Authentication Policy.

5.2.3. Authentication of organisation identity Confidentiality/Encryption Certificate

All organizations and entities entering into business agreements with Telstra Corporation, that make use of the Telstra Issuing CA, must comply with the provisions of this CPS and all subscriber agreements unless other business contracts specify a mutual non-compliance. A person authorized to act on behalf of a department or organization can make an application for the department or organization to become a Subscriber (i.e., device, application server, etc.).
Detailed naming standard and mechanism is discussed in a separate Telstra PKI Identification and Authentication Policy.

Digital Signature Medium Assurance and High Assurance Certificates are not intended

for use by current Telstra PKI. Where the technology does not permit the independent generation of Digital Signature and Confidentiality/Encryption key pairs, the Digital Signature key pair shall not be used.

5.2.4. Authentication of individual identity

This section is out of scope for current Telstra CA. Please refer to other Telstra specific CA CPS for these PKI use cases.

5.2.5. Initial Identity Validation

A subscriber (and/or certificate applicant) shall be an employee of the Telstra corporation, or other entity (contractor, device) that has an employment arrangement, contract, or other legally identifiable relationship with Telstra (as agreed to in the Telstra CA CPS), and is bound to comply with the provisions of employment and/or applicable Telstra corporate policies. The identity of the subscriber is based on the information available in the Telstra Corporation Corporate Directory. The vetting of the subscriber's identity will be performed as part of the certificate issuance process by an authorized Telstra employee (e.g. manager or application)

The Telstra CA shall rely on an existing business process to keep a record of the type and details of the identification used for the authentication of the organization (and associated responsible individual) for at least the life of the issued certificate.

6. CERTIFICATE LIFECYCLE MANAGEMENT

6.1. Certificate Management Process

Telstra CA Certificate Management Process within the Telstra PKI, and includes, for example:

1. Certificate registration and issuance
    a. enrollment (registration/application)
    b. signing request
2. Certificate deployment (& key pair generation)
3. Certificate renewal
4. Certificate revocation
5. Certificate Re-Key
6. Certificate Modification

6.1.1. Certificate Issuance

The procedures and requirements with respect to a certificate issuance are set out in this CPS. A request for a certificate does not oblige the Telstra Issuing CA to issue a certificate.

There are two principal types of applications for certificates:

1. CA certificates
2. Application server, device certificates

6.1.1.1. Server Certificate

A server certificate may be a certificate used for service or device authentication purposes. An authorised person (e.g., delegated administrator, applications administrator, hosting service, etc.) can acquire a server via Telstra PKI Dcerts process and procedures, detailed process and policy will be outlined in a separate PKI document). The applicant must provide the following information for the requesting server:

6.1.1.2. Individual (Secure Email) Certificate

This section is out of scope for the current Telstra PKI Issuing CA.

6.1.1.3. CA and RA Administrator, and Vetter Applicant

A request to acquire a CA or RA administrator, or vetter credentials will be made only by designated CA personnel. The detail of this topic will be out of scope for Telstra PKI CA CPS.

6.1.1.4. Non-verified subscriber information

Only information utilized for authenticating a subscriber certificate request will be verified; other information provided by the subscriber as part of the enrolment will be not be verified for accuracy. Telstra Corporation certificate authority reserves the right not to publish information that is not required for the responsible and secure operation of the Telstra CA, or issuance of the certificate. The Naming convention and conformity to the rules set forth in section 5.1 of this document as well as the identity and authentication information provided by subscribers will be considered in enrolment

6.1.1.5. Application for cross-certificate

This section is out of scope for the current Telstra Issuing CA CPS.

6.1.2. Enrolment process and responsibilities

Subscribers registering and accepting a certificate from the Telstra CA will be required to consent to a subscribers agreement or equivalent agreement consisting of:

1. Certification that identification information provided to Telstra Corporation

during a previous registration process is accurate.
2. Agreement to the protection of related keys and passwords, and if applicable, protection of tokens.
3. Agreement to the acceptable use and reliance on certificates as described in this CPS and relevant corporate service documentation.
4. Obligations to verify the selection of correct certificates prior to use.
5. Revocation obligations and processes.
6. Agreement to lifetime of certificates, and
7. Other disclaimers identified in the agreement.

6.2. Certificate Application Processing

6.2.1. Performing identification and authentication functions

The Subscriber shall be tightly bound to the public keys and the information submitted. The Telstra Issuing CA shall require that each application be accompanied by:

- Proof of identity and authorisation for any requested certificate attributes.
- Concurrence to a subscriber agreement or equivalent participation agreement of the applicable terms and conditions governing the applicants use of the certificate, and
- A properly formatted PKCS #10 or equivalent certificate request, including the public key.

In case the entity is a machine or object, the certificate request may be signed by a valid certificate pertinent to the authorised administrator or by the person responsible for the system or object.

6.2.2. Approval or rejection of certificate applications

Following the validation, Telstra Issuing CA shall notify a subscriber, directly or through the associated RA that the CA has created a certificate and provided the subscriber with access to the certificate. In case of rejection the Telstra CA shall notify the subscriber why the request was rejected.

6.2.3. Certificate Issuance

Upon successful completion of the subscriber identification and authentication process in accordance with this Policy, and complete and final approval of the certificate application, the CA shall issue the requested Certificate, notify the applicant thereof, and make the Certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or available for pickup by, the Subscriber only. A CA will not issue a Certificate without the consent of the applicant and, if applicable, the applicant's sponsor.

6.2.4. Actions during certificate issuance

Telstra CA issues certificates based on requests that are correctly formatted and properly verified according to Section 5.2 - Authentication. The issuance of a certificate by the Telstra CA indicates a complete and final approval of the certificate application by the CA. All certificate information transmitted electronically between the subscriber and the Telstra Issuing CA is protected by a secure process.

6.2.4.1. Notification to subscriber by the CA of issuance of certificate

A subscriber will be notified by the Telstra CA of the publishing of the subscriber’s certificate in a repository or confirmation of delivery of subscriber’s certificate. The issuance notification will be in the form of an email or a message (web page or pop-up window) to the subscriber informing of the successful completion of the enrolment process.

6.2.5. Certificate Acceptance

6.2.5.1. Conduct constituting certificate acceptance

Telstra Issuing CA does not require notification from an end user acknowledging acceptance of an individual certificate. Telstra considers the use of the certificate to constitute acceptance of the certificate. By accepting the certificate, the subscriber acknowledges:

- That the information contained in the certificate is true and correct
- That the applicant agrees to be bound by the rules of the Telstra Issuing CA as set forth in this CPS, and other existing agreements between Telstra Corporation and the Telstra employee, authorised vendor or agent.

Telstra CA however will require that a Subscriber acknowledge acceptance of a device or web server SSL certificate. There will be a 'formal' acceptance message from the person who is installing the device or SSL web certificates into the device or web server back to the Telstra Issuing CA.

6.2.5.2. Publication of the certificate by the CA

Telstra Issuing CA is responsible for repository and publication functions. Telstra Issuing CA shall publish certificates in a repository based on the certificate publishing practices of Telstra Issuing CA, as well as revocation information concerning such certificates, as defined in section 4 – Publication and Repository Responsibilities

6.2.5.3. Notification of certificate issuance by the CA to other entities

No notification of issuance or revocation will be provided to any other party when a certificate is issued or revoked except, in the case of revocation, through the issuance of a CRL.

6.3. Key Pair & Certificate Usage

6.3.1. Subscriber private key and certificate usage

The subscriber shall only use certificates, issued by Telstra CA, and their associated key pairs for the purposes identified in the Telstra CA CPS and in any relevant Telstra service documentation. Certificates and associated key pairs may only be used for approved purposes.

6.3.2. Relying party public key and certificate usage

Prior to using a subscriber's certificate, a relying party shall verify that the certificate is appropriate for the intended use.

6.4. Certificate Revocation & Suspension

6.4.1. Identification and authentication for Revocation request

Telstra CA shall authenticate a request for revocation of a certificate. A CA administrator or RA administrator will perform actual revocation and validate the reason for the revocation. An issuing CA shall keep a record of the type and details of the revocation request including the identity and authentication of the requesting person.

An End-Entity may request revocation of its certificate at any time for any reason.

Managers and officers of Telstra Corporation may also request the revocation of a current employee, terminated employee or 3rd party (business partner) at any time. The Telstra CA when faced with such a request will adopt authentication mechanisms that balance the need to prevent unauthorised requests against the need to quickly revoke certificates. Therefore, in the event the request is electronically submitted the identity of

the requestor may be authenticated on the basis of the digital signature used to submit the message. If the request is signed using the private key corresponding to the requestor's Public Key, such a request will be always accepted as valid.

Requests for certificate revocation must be accompanied by a verified (in writing or digitally) message according to Telstra Corporation business rules and practices. Requests by an authorised representative of the certificate holder's employer will always be accepted as valid certificate revocation and suspension.

6.4.1.1. Circumstances for Revocation

A certificate shall be revoked:

- When a subscriber fails to comply with obligations set out in the Telstra CA CPS, Subscriber agreement or applicable law.
- When the basis for any information in the certificate changes.
- A change in the business relationship under which the certificate was issued occurs.
- Upon suspected or known compromise of the private key, as evidenced by:
    - Missing cryptographic devices.
    - Tamper evident seals or envelope numbers or dates and times not agreeing with log entries.
    - Tamper evident seals or envelopes opened without authorization or showing signs of attempts to open or penetrate.
    - Indications of physical or logical access attempts to the certificate processing system by unauthorized individuals or entities.
- When a subscriber is no longer participating in a corporate application or service for which the certificate was issued, or no longer needs access to secured organizational resources.
- When the Telstra Issuing CA suspects that conditions may lead to a compromise of a Subscriber's keys or certificates, it may, in its discretion, revoke the Subscribers certificate.

6.4.1.2. Who can request Revocation

The revocation of a certificate may only be requested by:

- The individual, department or organization which made the application for the certificate.
- An authorised executive, supervisor or administrator (Telstra PKI policy management authority) on behalf of a **subscriber** or upon the Subscriber's termination.
- Personnel responsible for the operations of the Telstra Issuing CA.

6.4.1.3. Procedure for Revocation request

All requests for revocation shall be submitted via an on-line process or in writing. The Telstra Corporation Corporate Directory authenticated revocation request and any resulting actions taken by the CA shall be recorded and retained as required. In the case where a certificate is revoked, justification for the revocation shall also be documented.

Where a Subscriber certificate is revoked, the revocation shall be published in the appropriate CRL of the issuing CA. The CRL will be accessible in accordance to section 6.2.9.2 – CRL issuing frequency.

6.4.1.4. Revocation checking requirement for relying parties

Prior to using a certificate, a relying party shall check the status of all certificates in the certificate validation chain against the appropriate and current CRL in accordance with

the requirements stated in this section. As part of this verification process the digital signature of the CRL or OCSP response will also be validated. The CRL distribution point will be identified in every certificate.

6.4.1.5. CRL Issuing Frequency

The Telstra CA will issue a current CRL from the Issuing CA three weeks (or as required). In cases where a certificate is revoked, the Telstra Issuing CA will issue a new CRL immediately as per the requirements in Section 6.2.8.3 – Procedure for Revocation request. The Telstra Issuing CA will synchronise the CRL issuance and publishing to the account-01 LDAP directory and the Internet facing web server publishing to ensure the most recent CRL is available to Relying Parties.

6.4.1.6. Maximum latency for CRLs

The Telstra Issuing CA shall synchronize, automatically or manually, its CRL issuance with an accessible directory or web site to provide accessibility of the most recent CRL to relying parties. The latency for the publishing of the CRL will be immediate or as the supporting technology will support, generally it is within minutes.

6.4.1.7. On-line revocation/status checking availability

No stipulation.

6.4.1.8. On-line revocation checking requirements

No stipulation.

6.4.1.9. Other forms of Revocation advertisements available

No stipulation.

6.4.1.10. Special requirements Re key compromise

No stipulation.

6.4.2. Circumstances for Suspension

Generally, circumstances for a certificate to be suspended include:

- A revocation request has been received, but has not yet been authenticated or validated
- Long-term disability or other extended absence
- When there is uncertainty concerning the facts surrounding the motivating factors for revocation.

The Telstra Issuing CA will support certificate suspension for limited situations as determined by the Telstra Issuing CA. Suspension of a certificate will be handled by revoking a certificate and subsequent re-issuance of a certificate once the circumstance for suspension is no longer applicable. Re-issuance will consist of a new certificate request.

6.4.2.1. Who can request Suspension

A request for suspension can be requested by the personnel responsible for the operations of the Telstra Issuing CA., the subscriber, or by the subscriber's manager.

6.4.2.2. Procedure for Suspension request

The procedures for requesting a suspension are the same as for requesting revocation in Section 6.2.7.1.

6.4.2.3. Limits on Suspension period

Seven Days

6.4.3. Certificate status services

6.4.3.1. Operational characteristics

The CRL will be referenced by a PKI-enabled application to verify the validity of a certificate. The Telstra Issuing CA certificates include the CRL name and distribution points as part of the certificate extension information. When a certificate is revoked, the serial number of the certificate is added to the CRL.

Delta CRLs will keep a list of certificates that have been revoked since the last base CRL publication. The client caches a base CRL until the CRL's validity period has expired. To ensure the validity of a certificate, a client must receive the latest list of revoked certificates.

Once a certificate is revoked, a CRL will be immediately published following revocation, the CA database repository is updated with the revocation information. On an exception basis, CRLs may also be issued between these intervals (such as upon detection of a serious compromise situation).

The CRL access URL will also be provided in the detailed body of the certificate.

6.4.3.2. Service availability

Telstra Issuing CA will provide a current CRL that is accessible by Relying Parties and Subscribers for checking the status of all certificates in the certificate validation chain. The CRLs will be signed so that the authenticity and integrity of the CRLs can be verified.

Telstra Issuing CA may optionally provide On-line Certificate Status Protocol (OCSP) information services. Subscribers and Relying Parties who require such on-line certificate status services may check certificate status through the use of OCSP.

6.4.3.3. Optional features

No Stipulation

6.4.3.4. End of Subscription

The end of a subscription as a result of no longer requiring the service or compromise will result in the immediate revocation of the certificate and the publishing of a CRL or other certificate status verification system.

6.5. Certificate Renewal

Certificate renewal is the re-issuance of a certificate with a new validity date using the same public key corresponding to the same private key. A Subscriber may request issuance of a new Certificate for a new key pair from the CA that issued the original Certificate, provided the original Certificate has not been suspended or revoked.

6.5.1. Identification and Authentication for Re-key Requests

The Telstra Issuing CA shall require that a Subscriber, entity/person authorized to act on behalf of a department, organization or group, is currently in possession of a valid certificate and that they remain an employee or agent of Telstra Corporation that have an employment arrangement or contract with Telstra Corporation and are bound to comply with the provisions of employment and applicable corporate policies.

Any additional Subscriber information provided shall be complete and validated with full disclosure of all required information in connection with a certificate renewal.

6.5.2. Processing certificate renewal requests

The Subscriber shall be tightly bound to their public keys and the information submitted. The Telstra Issuing CA shall require that each renewal be accompanied by:

- Proof of identity and authorization for any requested certificate attributes; and
- Continued concurrence to a subscriber agreement or equivalent participation agreement of the applicable terms and conditions governing the applicant's use of the certificate.
- Renewal of an affiliated individual shall require verification that the affiliation still exists.
- An Entity requesting re-key may authenticate the request for re-key using its valid Digital Signature key pair.

Where the keys have expired, the request for re-key must be authenticated in the same manner as the initial registration.

On a case by case basis, certificate renewal may be permitted when information in a certificate has changed.

6.5.3. Conduct constituting acceptance of a renewal certificate

Telstra Issuing CA does not require notification from an end user acknowledging acceptance of an individual certificate. Telstra considers the use of the certificate to constitute acceptance of the certificate. By accepting the certificate, the subscriber acknowledges:

- That the information contained in the certificate is true and correct
- That the applicant agrees to be bound by the rules of the Telstra Issuing CA as set forth in this CPS, and other existing agreements between Telstra Corporation and the Telstra employee, authorized vendor or agent

Telstra Issuing CA however will require that a Subscriber acknowledge acceptance of a device or web server SSL certificate. There will be a 'formal' acceptance message from the person who is installing the device or SSL web certificates into the device or web server back to the Telstra Issuing CA.

6.5.4. Publication of the renewal certificate by the CA

Telstra Issuing CA is responsible for repository and publication functions. Telstra Issuing CA shall publish certificates in a repository based on the certificate publishing practices of Telstra Issuing CA, as well as revocation information concerning such certificates, as defined in section 4.

6.5.4.1. Notification of certificate issuance by the CA to other entities

No notification of issuance or revocation will be provided to any other party when a certificate is issued or revoked except, in the case of revocation, through the issuance of a CRL.

6.6. Certificate Re-Key

6.6.1. Circumstance for certificate Re-key

This use case applies to the processes of Certificate Issuance and Renewal.

6.6.2. Re-Key after revocation – No Key Compromise

No stipulation.

6.6.2.1. Re-Key after revocation – Key Compromise

No stipulation.

6.6.3. Special requirements Re-key compromise (CA Signing keys)

No stipulation.

6.6.3.1. Who may request certification of a new public key

No stipulation.

6.6.4. Processing certificate re-keying requests

No stipulation.

6.6.4.1. Notification of new certificate issuance to subscriber

No stipulation.

6.6.4.2. Conduct constituting acceptance of a re-keyed certificate

No stipulation.

6.6.4.3. Publication of the re-keyed certificate by the CA

No stipulation.

6.6.4.4. Notification of certificate issuance by the CA to other entities

No stipulation.

6.7. Certificate Modification

6.7.1.1. Circumstance for certificate modification

A certificate may be modified:

- When the authenticated certificate information has minor changes, for example, the subject email address update or non-essential parts of names or attributes changes.
- A change in the business relationship under which the certificate was issued occurs.

6.7.1.2. Who may request certificate modification

The modification of a certificate may only be requested by:

- The individual, department or organisation which made the application for the certificate.
- An authorized supervisor or administrator (Delegated Administrator) on behalf of a Subscriber; or
- Personnel of the Telstra CA.

6.7.1.3. Processing certificate modification requests

All requests for certificate modification shall be submitted via an on-line process or in writing. The authenticated modification request and any resulting actions taken by the Telstra CA shall be recorded and retained as required. The detailed processes are outlined in other relevant PKI documentations.

6.7.1.4. Notification of new certificate issuance to subscriber

The issuance notification will be in the form of an email or a message (web page or pop-up window) to the Subscriber informing of the successful completion of the modification/renewal process.

6.7.1.5. Conduct constituting acceptance of modified certificate

Telstra CA does not require notification from an end user acknowledging acceptance of a modified certificate (new certificate). The acceptance of the certificate by the subscriber is manifested by changing the default pass phrase of the token containing the certificate and

key pair, and subsequent utilization of the new certificate.

Telstra CA will require that an entity acknowledge acceptance of a device or web server SSL certificate modification. There will be a 'formal' acceptance message from the person who is installing the device or SSL web certificates into the device or web server back to the Telstra Issuing CA's.

6.7.1.6. Publication of the modified certificate by the CA

Publication of a modified certificate will be as the initial publishing of the certificate.

6.7.1.7. Notification of certificate issuance by the CA to other entities

No notification of renewal will be provided to any other party when a certificate is modified.

6.7.2. Key escrow and recovery

6.7.2.1. Key escrow and recovery policy and practices

Depends on the different Telstra PKI use cases, end user encryption private keys may be recoverable via Key Escrow.

6.7.2.2. Session key encapsulation and recovery policy and practices

No stipulation.

7. FACILITY MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

7.1. Physical Security Controls

The following physical security controls shall be in place prior to initial operation of the Telstra CAs. Subscribers shall satisfy the security requirements as documented in this CPS prior to certificate issuance.

The Telstra Root CAs are housed in a secure environment protected by multiple levels of security with full-time personnel on duty 7 days per week, 24 hours per day. Personnel are assigned responsibilities to monitor the security and integrity of the PKI service operations and to maintain appropriate records as needed.

7.1.1. Site Location and Construction

The Telstra Corporation Limited Root CA is housed in a Secure Facility in Telstra Secured data centre. The Secure Facility is staffed on a 24 x 7 basis.

- The Telstra CA's are to reside in a physically secure environment.
- To support the objective of protecting against intrusions, the physically secure environment will consist of:
    - Dedicated computing centre with true floor to ceiling walls,
    - Physical security requiring two-person control, to gain access into the secure cabinet containing the Telstra Root CA.
- One or more surveillance cameras will provide continuous monitoring of entry and exit to the physically secure environment. Under no circumstances should surveillance cameras be configured to allow the monitoring of computer screens, keyboards, PIN pads, etc. Activation of the recording function will either be continuous or be done via a motion detector, which is separate from the physical intrusion detection system. Continuous lighting must be available for the cameras.
- The physically secure environment will have an intrusion detection system:
    - The intrusion detection system must have 24-hour monitoring.
    - The system will be capable of recording and archiving alarm activity.
    - Alarm activity will include unauthorized entry attempts or any deliberate or inadvertent actions that disable the intrusion detection system.
    - All logged alarm activity information will be reviewed and resolved.
- Entrance to the Computer Room will require the use of individual access proximity cards.
- Physical keys and combination locks when used as the access control mechanism:
    - Physical keys to locks shall be marked so that each individual key can be identified,
    - Assigned to an individual employee, controlled and later audited if necessary.
    - The distribution and collection of keys shall be recorded. A record of individual access for each key will be maintained in a central database or repository.
- When a PIN or password is recorded, it shall be stored in a security container accessible only to authorized personnel.
- There is programmed maintenance currently in place for access control systems. The analysis/results of the programmed maintenance can be made available to support audit requirements.

- All access control and monitoring systems must be tied to a UPS, The UPS system must:
  - Be inspected at least annually,
  - The inspection documentation must be retained for at least a one-year period.
- All RA sites or RA workstations used for on-line Entity management with the CA must be located in areas that satisfy the following controls:
  - Activity is monitored by the personnel, who work there, by other personnel or by security staff.
- Entry beyond the reception area is indicated by a recognizable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment.
- all media securely protected when unattended, or
- access is limited to personnel who work there.
- Monitored manually or electronically for unauthorized intrusion at all times.
- Ensure all removable media and papers containing sensitive plain text information are stored in secure containers.

7.1.2. Physical Access

The Telstra CA (Root CA) system is located in a cabinet in a secure environment which supports multiple secure applications. The access to the secure environment is restricted to authorized personnel only. The cage housing the Telstra CA's is a locked enclosure with dual control authentication to which only PKI service operational authority personnel have physical access. The class B cabinet containing the CA system is designated a two-person zone, and appropriate controls are deployed to assure that no one person has access to the cabinet alone.

The CA facility includes the following security measures:

- The facility entrance is locked at all times whether occupied by CA employees or unoccupied.
- The facility is within a building constantly monitored by full-time security personnel.
- The facility is protected by intrusion detection systems at all times including:
  - Video monitoring by physical security personnel at all times to include monitoring of the facility, the entrance, and the secure storage containers.
- Alarmed entry when facility is unoccupied.
- Alarmed motion detectors when the facility is unoccupied.

A facility security check for physical tampering is performed periodically to ensure that:

- All equipment is in the proper state for the current mode.
- All physical security systems are functioning properly.
- All safes and security containers are properly secured.
- The CA facility and surrounding area are secure against unauthorized access.

All removable hardware cryptographic modules are stored in lockable containers when not in use.

Telstra Issuing CA personnel with access to the physically secure environment will not have access to the VCR tapes or digital images. Procedures must exist for the granting and revocation of access privileges to individuals.

7.1.2.1. CA Physical Security Logs

- Logs of access will be reviewed regularly and the review must be documented.
- All access granting, revocation, and review procedures must be documented.
- CA employees (authorized individuals with a formal PKI role) having access

to the physically secure CA are logged by the access control system. This record includes
    - Date and time in and out,
    - Identification of individual,
- Visitors (contractors, maintenance personnel, etc.) to the CA facility are to be escorted by authorized individuals and sign an access logbook. This log is maintained within the CA server room. This logbook will include:
    - Name and signature of visitor,
    - Participants Organization,
    - Name and signature of individual escorting the visitor,
    - Date and time in and out,
    - Reason for visit.
- Significant alarm events will be documented. Under no circumstances shall an individual sign-off on an alarm event in which they were involved.
- The use of any emergency entry or exit mechanism will cause an alarm event.
- A process exists for synchronizing the time and date stamps of the access, intrusion detection and monitoring (camera) systems to ensure accuracy of logs. This is be done by either automated or manual mechanisms.

7.1.2.2. Subscriber Physical Security Controls

Subscribers shall provide the necessary protection to their private keys whether in use or not. Private and secret keys must not be in human comprehensible form to any person at any time.

Subscribers, such as devices and application server, that contains private keys on a hard drive (software generated) shall be physically secured or protected with an appropriate boot level or suitable authentication access control.

7.1.3. Power and Air Conditioning

All Secure Facilities are connected to a standard power supply. All critical components are connected to uninterruptible power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure.

The Secure Facility has an air conditioning system which controls temperature and humidity. Backup air conditioning units are provided for the no lone zones (i.e. the CA room).

The PMA will ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system.

7.1.4. Water Exposures

The Secure Facility is protected against water exposure by being located on built in raised floors of a building that is not in a flood zone.

7.1.5. Fire Prevention and Protection

The Secure Facility is subject to normal Telstra Corporation Limited fire prevention and protection procedures.

Early detection of smoke in the Secure Facility is assured through the use of an extremely sensitive VESDA (Very Early Smoke Detection Apparatus) smoke detection system which continuously samples air from under the computer room floor and from the computer room itself. On detection of an unacceptably high level of smoke in the sampled air, the VESDA unit triggers a non-toxic gas fire suppression system.

In addition to this automatic fire suppression system, suitable fire extinguishers are maintained in the secure operating area.

The Secure Facility's proximity swipe-card system supports emergency evacuation

procedures to cater for environmental hazards such as fire, natural disasters and structural collapse.

7.1.6. Media Storage

All magnetic media containing sensitive Telstra PKI information, including backup media, is stored in data protection containers in cabinets or safes with fire protection capabilities which are located either within the secure operating area or in a secure off-site storage area.

The Telstra Issuing CA ensures that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

7.1.7. Waste Disposal

Waste disposal at the Secure Facility

Waste Disposal Sensitive waste material or PKI information SHALL be shredded and destroyed by an approved service. Removable media containing sensitive information SHALL be rendered unreadable before secure disposal. Cryptographic devices, smart cards, and other devices that may contain Private Keys or keying material SHALL be physically destroyed or zeroized in accordance with the manufacturers' waste disposal guidelines.

7.1.8. Off-Site Backup

The CA service equipment is backed up on a periodic basis and the backup copies are stored securely at an off-site location, to recover from a system failure. The security at these locations prevents unauthorized and un-audited access to backup data or media.

The off-site storage:

- Has appropriate levels of physical security in place; and may be accessed on a 24 x 7 basis by authorised personnel for the purposes of retrieving software and data.
- The Of-Site Safe is a dual custody fire proof unit

7.2. Procedural Controls

7.2.1. Trusted roles

The Telstra PKI contains a number of designated 'positions of trust'. These positions underpin the secure and reliable operation of the Telstra PKI, and as such must be filled by competent and trustworthy people (although the same person may fill several positions of trust when required).

The general principle is that any role providing an opportunity to compromise private key material or impact on the certificate life cycle must be a trusted role. Further details are set out in documentation not publicly available.

The Telstra Issuing CA requires a separation of duties for critical CA functions to prevent one person from maliciously using a CA system without detection. The practice referred to as split knowledge and dual control. Telstra Issuing CA employee's access to the CA systems is to be limited to those actions they are required to perform in fulfilling their responsibilities. These responsibilities shall be well understood by the Telstra PKI employees.

There is a separation of duties and two-person control required for specific activities, such as:

- Generation of new CA key pair,
- Replacement of the CA private signing key and associated certificate,
- Change in the certificate profile security policy.

All CA administrators and RA administrators will be individually accountable for their actions. This will be accomplished by a combination of physical, electronic and policy controls:

- Restricted access to facility – entry is monitored both entry and exit,
- Audit logs will record administrator log-in and log-out of operating system,
- Audit logs will record administrator log-in and log-out of CA,
- Audit logs will record certificate creation and revocation. (See Section 5.4.1),
- Technical controls that enforce dual access
- Policy and procedural controls that require dual access

Note: As defined in ISO 9564-1, split knowledge is "a condition under which two or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key". The resultant key exists only within "secure cryptographic devices". Dual control is explained in the standard as "a process utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information, whereby no single entity is able to access or utilize the materials, e.g., cryptographic key".

7.2.1.1. CA Administrator

This is a role within Telstra PKI team with the ability to configure, and maintain the CA, including backup and recovery operations, and audit functions. It also includes the ability to assign all other CA roles and renew the CA certificate. This role will be staffed by a Telstra PKI Policy Management Authority authorized Telstra employee.

CA Administrator:

- Configuration and maintenance of the CA system hardware and software,
- Commencement and cessation of CA services,
- Management of PKI Operators and other PKI Officers,
- Configuring CA security policies,
- Verification of audit logs,
- Verification of CPS compliance.

7.2.1.2. Certificate Manager

Certificate Managers typically have responsibility for managing a group of Certificate Subscribers and potentially their smart card tokens. A certificate manager will conduct certificate management functions for a group of users for which they have been granted permissions to manage. The certificate manager functions include user management, approving certificate requests, recovery of user's keys, revocation of certificates, and renewal of certificates. The Certificate Manager Role is staffed by a Telstra PKI PMA authorized personnel.

7.2.1.3. Auditor

This is a role within Telstra PKI with the ability to configure, and maintain all CA audit data, including backup and recovery of audit data, and audit related functions. This role will be staffed by an authorized Telstra employee.

7.2.1.4. Operating System Administrator

The operating system hosting the Telstra CA systems shall require a separation of duties for system-level tasks to prevent one person from maliciously using the CA server operating system without detection. Operating System Administrator access to the CA systems is to be limited to those actions they are required to perform in fulfilling their systems management responsibilities. These responsibilities shall be well understood by the Operating System Administrators. The Operating System Administrator cannot be a person that is also filling a CA Administrator or Auditor role.

7.2.1.5. RA trusted roles

The Telstra Issuing CA will ensure that RA personnel understand their responsibility for the identification and authentication of prospective Subscribers and perform the following functions:

- acceptance of subscription, certificate change, certificate revocation and key recovery requests,
- verification of an applicant's identity and authorizations,
- transmission of applicant information to the CA,
- Provision of authorization codes or other initialization data for on-line key exchange and certificate creation where applicable.

The Telstra Issuing CA may permit all duties for RA functions to be performed by one individual.

7.2.2. Number of persons required per task

The Telstra CA's will implement the principle referred to as "split knowledge and dual control", such that no single individual may perform CA activities. In particular, the Telstra CA's shall implement "m of n" access. The "m" must be at least two (2), and the "n" must be no less than four (4), whereby at least two people are required to start a CA and activate a CA signing key. Multi-user control is required for CA key generation.

Telstra CA shall have a verification process that provides an oversight of all activities performed by privileged CA role holders. That is roles that can issue certificates, generate keys, and administer the CA configuration settings.

Multi-person control is used where the requirement is to provide enhanced security and checks and balances over Telstra PKI operations. In particular:

- The appropriate Security Manager always remains separate from the Telstra PKI System Operators in order to provide an independent third party when reviewing and auditing Telstra PKI Operations,
- logical access controls for Telstra PKI operations personnel have been implemented to ensure that no one person can access a single machine and therefore the sensitive information contained on those machines;
- the CA Operators are broken into the following 2 groups:
  - Group 1 - has access to the logon passphrase for cryptographic elements; and
  - Group 2 - has access to the logon database applications, and
- Any task requiring the creation, backup or import into a database of a Telstra PKI component private key takes place in a no-lone zone and therefore involves two trusted persons, one performing the function and the second person fulfilling a security monitoring role.
- Telstra CA will ensure that no single individual may gain access to Subscriber private keys stored by the CA. At a minimum two individuals, preferably using a split knowledge technique, such as twin passwords or certificates, must perform any key recovery operation. Telstra Issuing CA will ensure that any verification process it employs provides for oversight of all activities performed by privileged CA role holders.

7.2.3. Identification and authentication for each role

All Telstra Issuing CA personnel, involved in the operation of the Telstra PKI, shall have their identity and authorization verified before they are:

- Included on the access list for the CA facility,
- Included on the access list for physical access to the CA system,
- Given credentials/accounts for the performance of their CA operation's role; these certificates and accounts shall:

- Be directly attributable to an individual,
- Not be shared, and
- Be restricted to actions authorized for that role through the use of a combination of CA software, operating system and procedural controls.

CA operations will be secured, using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network.

7.2.4. Roles requiring separation of duties

Telstra CA shall require a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection. This is applicable to all CA Administrators.

To enhance security of the Telstra PKI the following roles are to be undertaken by different personnel:

- the Telstra PKI hosting facility Security Administrator will normally remain separate from the Telstra PKI System Operators in order to provide an independent review of audit logs unless in exceptional circumstances (i.e. personnel issues whereby integrity of the Telstra Corporation Limited PKI service being operated could be breached).

7.3. Personnel Security Controls

Telstra CA requires that all personnel performing duties with respect to the operation of a CA or RA 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 comprehensive training with respect to the duties they are to perform,
- be bound by statute or contract not to disclose sensitive CA security-relevant information or Subscriber information, and
- Not be assigned duties that may cause a conflict of interest with their CA or RA duties.

7.3.1. Background, qualifications, experience and clearance requirements

The Telstra Issuing CA requires that all personnel performing duties with respect to the operation of Telstra PKI have sufficient qualification and experience. All personnel must meet organizational personnel security requirements and CA Administrators shall have the following:

- PKI knowledge and training
- Security training
- Product specific training, and
- No major observations in the background check verification.

The Telstra Issuing CA will formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this policy.

7.3.2. Background check procedures

All background checks will be performed in accordance with Telstra Corporation standard organizational policies and procedures. All personnel considered for employment are thoroughly screened by a reputable investigative agency/or a department within Telstra Corporation authorized to perform checks such as:

- Criminal background verification,
- Verifiable employment history.

PMA shall conduct an appropriate investigation of all personnel who serve in trusted roles periodically thereafter as necessary, to verify their trustworthiness and competence in accordance with the requirements of this CPS and CA's personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role. The PMA may establish additional requirements conforming to state law and policy.

7.3.3. Training requirements

Telstra CA may provide comprehensive training for all PKI personnel performing duties with respect to the operation of the Telstra Issuing CA. Such training will consist of at least:

- IT Security and General PKI knowledge,
- CA administration and operation, and
- CA disaster recovery processes,
- basic Telstra PKI concepts,
- the use and operation of the all Telstra PKI software versions in use on the system,
- Telstra PKI hosting facility procedures, computer security awareness and procedures, and
- The meaning and effect of this Telstra Issuing CA CPS.

A formal training program, founded on competency-based training principles shall be in place. The Telstra PKI Team Leader is responsible for ensuring that new and inexperienced personnel are appropriately trained and supervised.

7.3.4. Retraining frequency and requirements

The requirements for Section 7.3.3 shall be kept current to accommodate changes in a CA system (software and procedures). Refresher training shall be conducted as required, and management shall review these requirements once a year.

The introduction of any new security procedure or major software release will be accompanied by a corresponding education program for personnel affected by the changes to ensure that they are aware of their new responsibilities.

Remedial training is completed when recommended by audit findings and / or recommendations.

7.3.5. Job rotation frequency and sequence

In the event that there is job rotation, all passwords will be changed, appropriate certificates revoked and reissued, user IDs deleted and recreated. There is NO sharing of passwords or accounts.

7.3.6. Sanctions for unauthorised actions

All employees of the Telstra Issuing CA are employees/contractors (where deemed allowed) of Telstra Corporation. Therefore, all PKI employees are expressly bound by existing employment agreements, as well as applicable corporate policies. The sanctions for unauthorized actions by Telstra Issuing CA employees are described in those documents.

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of the Telstra Issuing CA, Telstra Corporation PKI PMA will suspend the person's access to the Telstra PKI immediately until an investigation is conducted by Telstra Corporation Limited CSI. At the discretion of Telstra Corporation PMA, Telstra Corporation executives, and in accordance with the relevant Commonwealth legislation, (Criminal sanctions apply for contravention of relevant

legislation, for example the Crimes Act 1914 (Commonwealth), and the Public Services Act 1999 (Commonwealth)), further action may be recommended regarding employment status.

Depending on the nature of the actions sanctions may range from counselling and/or suspension of access rights, through to dismissal and/or legal action.

The Telstra Issuing CA may revoke all applicable certificates when a Subscriber fails to comply with obligations set out in this CPS, any agreement and/or applicable law. The Telstra Issuing CA may revoke a certificate at any time if it suspects that conditions may lead to a compromise of keys or certificates.

Prohibited actions in the Telstra PKI include (but are not limited to):

- Connecting private computers, computer peripherals, or computer software to the Telstra PKI network,
- Installing unauthorised software (including copyright infringed items). All software installations must be in accordance with the requirements of Telstra PKI policies and the documented change management procedures,
- Using Telstra PKI systems for unauthorised purposes, having diagnostic tools (capable of testing or breaking security resident in any system) on their machines, and
- Changing the configuration of any Telstra PKI hardware or software without approval of the Telstra PKI Security Administrator and the Telstra PMA.

7.3.7. Contracted Personnel - Management and responsibilities

All CA specific roles must be performed by Telstra employees or contractors who are subject to same level of background checks and HR policies as Telstra employees.

Casual Telstra PKI personnel and third party users who are not already covered by an existing contract including confidentiality clauses will be required to sign a Confidentiality Deed before being granted limited access to information processing facilities. The need for the party to enter into the Confidentiality Deed is at the discretion of Telstra Corporation PMA.

Contractors in breach of security obligations may be guilty of certain criminal offences, for example offences relating to computers, offences relating to espionage and official secrets and offences against the Government, as set out in the Crimes Act 1914 (Commonwealth) and other Commonwealth legislation.

7.3.8. Documentation supplied to personnel

The Telstra Issuing CA will make available to its employees/contractors documentation required by personnel to perform their duties, these include but are not limited to:

- All relevant hardware and software documentation,
- Any specific procedures, documents and contracts relevant to their position
- Application manuals where appropriate,
- Disaster Recovery Plans,
- Policy documents, including this CPS,
- Subscriber Agreements

Note: the Telstra PKI is largely composed of commercial-off-the-shelf products. Software documentation is therefore widely available to Telstra PKI personnel. General documents relating to the operation of the Telstra PKI such as this Telstra Issuing CA CPS, are available to Telstra Corporation Limited personnel, for example through publication on the Telstra Corporation Limited intranet or to the public through the Telstra Corporation Limited website. http://telstra-pki.pki.telstra.com.au/cps/

7.4. Audit Logging Procedures

Audit log files are generated for all events relating to the security of the Telstra Issuing CA. Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism will be used. All security audit logs, both electronic and non-electronic, will be retained and made available for compliance audits and legal review as required by the Archives Act 1983 (Commonwealth).

Contracted service providers for the CAs and or RAs will be contractually bound to comply with the Archives Act 1983.

7.4.1. Types of Events Recorded

All security type events including physical and logical access, process or configuration changes, generating keys, creating certificates, key usage, and any other event that may be required for auditing purposes will be recorded. The types of events are broken into two categories:

- Physical events such as Data Centre facility, computer room and CA enclosure access; Physical events may use electronic recording and/or logbooks.
- Logical events such as operating system operations and CA system operations. Logical events will be recorded automatically in audit logs at the operating level and application level.

7.4.1.1. Physical Events

For Physical events the following information will be recorded:

- Date and time of event,
- Identity of entity/entities,
- Purpose for access (i.e. maintenance, upgrades, enhancements, etc.)
- Any other requirements that provide information pertaining to the event (could be comments regarding the replacement of a disk drive as a result of a failure)

The following physical events will be recorded:

- Access room entry and exit;
- Alarm activation;
- Equipment sign-out and return; and
- CA system access.

7.4.1.2. Logical Events

Logical events are divided into operating system and CA system events. For both events the following will be recorded in the form of an audit record.

- Type of event (application, system security, etc.)
- Date and time the event occurred,
- Success or failure of event,
- Identity of the entity and/or operator of the CA that caused the event; and
- Any details about the event (may be error information or login message type information) Audit information will be kept, and whenever practical, audit logs will be digitally signed to maintain integrity of the information.

7.4.1.2.1 Operating System

All login activity will be logged to the system logs or separate access log file. All system-level activity (root-level activity or equivalent) will be logged, as appropriate, by either the operating system's logging facility or the access control application.

The following list represents audit events that will be monitored under the operating system for both successes and failures.

- Successful and unsuccessful logon events
- Privilege use and escalation of role/account
- System events:
- Critical events
- Emergency events
- System restarts

7.4.1.2.2 CA System

CA System event logging lists the events that will be monitored in the CA system. The following events monitored will be logged for both success and failure:

- CA audit Groups
- Back Up and Restore the CA Database
- Change CA Configuration
- Change CA Security Settings
- Issue and Manage Certificate Requests
- Revoke Certificates and Publish CRLs
- Store and Retrieve Archived Keys
- Start and Stop Certificate Services
- Back Up and Restore the CA Database
- Change CA Configuration
- Add/Remove Templates to the CA
- Configure the CRL Publication Schedule
- Modify Request Disposition for the Policy Module
- Modify Publish Cert Flags for the Exit Module
- Configure CRL Distribution Points (CDP)
- Configure Authority Information Access (AIA)
- Change the Policy Module
- Change the Exit Module
- Configure Key Archival and Recovery (KAR)
- Change CA Security Settings
- Configure CA Roles for Role-Based Administration of the CA
- Configure Restrictions on Certificate Managers
- Configure CA Auditing
- Issue and Manage Certificate Requests
- Incoming Certificate Requests
- Certificate Issuance
- Certificate Import
- Deletion of Rows in the CA Database
- Revoke Certificates and Publish CRLs
- Certificate Revocation
- CRL Publication
- Store and Retrieve Archived Keys
- Archival of Subject Keys
- Retrieval of Subject Keys
- Start and Stop Certificate Services
- Starting Certificate Services
- Stopping Certificate Services

7.4.1.3. Consolidation requirements

Information pertaining to the Telstra Issuing CA on the following will be collected, consolidated and reported either electronically or manually:

- System configuration changes and maintenance;
- Personnel changes;
- Discrepancy and compromise reports;
- Correspondence with CA related external parties such as software and hardware suppliers and network providers as it relates to system maintenance;
- Destruction of media containing key material, activation data, or personal Subscriber information.

7.4.2. Frequency of processing log

At a minimum, a review of audit logs will be conducted once every 30 days. All significant events shall be explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken following these reviews shall be documented.

7.4.3. Retention period of audit log

The Telstra Issuing CA shall retain its audit logs for at least one year (prior to being archived) and will retain audit logs in a manner described in Archives Act 1983 (Commonwealth).

7.4.4. Protection of audit log

Telstra Issuing CA system configuration and procedures will be implemented together to ensure that:

- Only authorized people have read access to the logs;
- Only authorized people may archive or delete audit logs; and,
- Audit logs are not modified.

The electronic audit log system shall include mechanisms to protect the log files from unauthorized viewing, modification or deletion. The entity performing audit log archive should not have modification rights and procedures will be implemented to protect archived audit data from deletion or destruction prior to the end of the audit log retention period. Audit logs shall be moved to a safe, secure storage location separate from the Telstra Issuing CA primary location

Manual audit information shall be protected from unauthorized viewing, modification or deletion. These logs shall also be placed in a secure area.

7.4.5. Audit collection system (internal vs. external)

The Telstra Issuing CA records and files are under the control of an automated collection system that cannot be modified by any application, program, or other system function. Any modification to the audit collection system is itself a recordable event.

Access to the building, room and enclosure where the CA system is stored and used will be monitored. Part of the monitoring may be recorded on video.

Operating System audit processes will be invoked at system start-up and cease only at operating system shutdown. CA System audit processes will be invoked at CA application start-up and will cease only at CA system application shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the Telstra Issuing CA shall determine whether to suspend CA operations until the problem has been rectified.

The audit collection system is both manual and automatic.

Event Collection Point	Automatic / Manual	Recording Entity
CA Facility	Automatic / Manual	Proximity cards, video, Electronic lock with logging, log sheets
Operating System • System Log • Security Log	Automatic	Operating System
CA System • Web Server logs • Log Server logs	Automatic	Certification Authority software

7.4.6. Notification to event-causing subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual or entity that caused the event.

7.4.7. Vulnerability assessments

Events in the audit process are logged, in part, to monitor inappropriate behaviour, system vulnerabilities and/or compromises. Telstra Issuing CA shall perform a vulnerability assessment, make appropriate recommendations to resolve issues and take appropriate action, as required.

7.5. Records Archival

7.5.1. Types of records archived

Telstra Issuing CA archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA.

At a minimum, the following data shall be recorded for archive:

- Telstra Issuing CA accreditation (if applicable)
- Certification Practice Statement (each version)
- Contractual obligations
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- Revocation requests
- Subscriber identity Authentication data
- Documentation of receipt and acceptance of certificates
- Documentation of receipt of tokens
- All certificates issued or published
- Record of a Re-key
- All CRLs issued and/or published
- All Audit Logs
- Other data or applications to verify archive contents
- Documentation required by compliance auditors

7.5.2. Retention period for archive

The minimum retention period for archive data is 7 years from the date of its creation. Specific customer information will be disposed of according to disposal standards. Audit and other information relative to the operations and continuity of the CA will be kept. Files are maintained online as deemed appropriate by Telstra Issuing CA.

Archives are retained for a period of seven years from date of generation in accordance with the requirements of the Archives Act 1983 (Commonwealth).

7.5.3. Protection of archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. The contents of the archive shall not be released except as determined by the Telstra Issuing CA or as required by law. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the Telstra Issuing CA location.

The automated archive system shall include mechanisms to protect the archived files from unauthorized viewing, modification or deletion.

Manual archived information shall be protected from unauthorized viewing, modification or deletion.

Documents that have reached their end-of-life will be destroyed following proper disposition rules based on the classification of the document. For sensitive or confidential paper documents, the documents will be securely disposed. Any certificate, audit, or control information on paper is considered confidential and will be shredded. Public documents may be placed in the disposal without shredding.

7.5.4. Archive backup procedures

Backup copies of the archives are created and maintained in case of the loss or destruction of the primary archives. Archive files are backed up on a daily basis. Backup files are stored at a secure and separate geographic location, on a weekly basis.

Audit trail files will be archived by the system administrator or script on a weekly basis. All files including the latest audit trail file will be stored in a secure archive facility. As part of the scheduled system back up, audit trail files will be backed up to media on a daily basis.

7.5.5. Requirements for time-stamping of records

All documents archived pursuant to this section shall be marked with the date of their creation or execution.

7.5.6. Archive collection system (internal or external)

The archive collection system may be a combination of both manual and automatic. The collection system will involve physical security as part of the collection of audit information.

7.5.7. Procedures to obtain and verify archive information

Telstra Issuing CA shall verify the integrity of the archives at least once every 12 months. Material stored off-site shall also be verified at least every 12 months for data integrity

7.5.8. Secure maintenance of Keys

Telstra Corporation Limited retains copies of the Public and Private Keys of the Telstra Issuing CA and subordinate SCAs in a Secure Facility.

7.6. Compromise and Disaster Recovery

The certification authority facility used by the Telstra Issuing CA has a disaster recovery/business continuity plan in place for providing certification authority services in accordance with this CPS.

7.6.1. Incident and compromise handling procedures

Incident and compromise handling procedures will be provided in Telstra Corporation Breaches of Security policy.

7.6.2. Computing resources, software, and/or data are corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to the responsible DRP manager and incident handling procedures are to be enacted immediately. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, disaster recovery procedures will be enacted.

7.6.3. Entity private key compromise procedures

In the situation that the Private Key is compromised, for whatever reason, the procedures outlined for a termination of the entity whose Private Key was compromised, would be followed. The Telstra PMA shall be notified as soon as practicable:

- All subscribers shall be notified as soon as practicable; and
- Further action determined by the Telstra PMA shall be implemented.

In the event of the compromise of a CA's digital signature key, prior to re-certification within the Telstra PKI, a CA must:

- request revocation of cross-certificates issued to the CA,
- revoke all certificates issued using that key,
- provide appropriate notice

After addressing the factors that led to key compromise, the CA may:

- generate a new signing key pair,
- Re-issue certificates to all entities and ensure all CRLs are signed using the new key.

In the event of the compromise, or suspected compromise, of any other entity's digital signature key, the entity must notify the issuing CA immediately. Subscriber key compromise will result in immediate revocation. The Telstra issuing CA must ensure that it's CPS and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

7.6.4. Business continuity capabilities after a disaster

Telstra Issuing CA has provided business continuity procedures in a business continuity plan which outlines disaster recovery procedures that outline the steps to be taken in the event of corruption or loss of computing resources, software and/or data.

7.6.5. Entity public certificate is revoked (Key compromise plan)

In the event of the need for revocation of a Confidentiality/Encryption certificate, the Telstra CA will include the Certificate serial number on an appropriate CRL. The Telstra CA has in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key.

7.7. Telstra PKI Termination

Telstra Corporation Limited may terminate the Telstra PKI at its own discretion or as directed by the Commonwealth government.

If the Telstra PKI is terminated, details of transition plans and procedures will be provided to Telstra PKI participants in a timely manner.

7.7.1. CA or RA termination

If Telstra Issuing CA ceases to operate as a CA:

- All certificates issued by the CA service will be revoked,
- All end entities will be notified within 7 days,
- All CA private keys will be destroyed to prevent compromise or fraudulent use.
- An archive of the CA database will be retained by the PKI service for a minimum of 7 years.
- The CA shall arrange for the continued retention of all CA keys, final CRL and other relevant information.

8. TECHNICAL SECURITY CONTROLS

8.1. Key Pair Generation and Installation

8.1.1. Key pair generation

Telstra CA key pair generation will be from a Secure Cryptographic Hardware Security Module (HSM) rated at least FIPS 140-2, level 3. Subscriber key pair generation will be supported in either hardware or software as stipulated in section 8.1.6.

The self-generated Telstra Issuing CA Private Keys do not require delivery.

The SCAs PKCS#10 Certificate request will be transferred to the Telstra Corporation Limited RCA in a way that ensures that:

- it has not been changed during transit;
- the sender possesses the private key that corresponds to the transferred public key; and
- The sender of the public key is the legitimate user claimed in the certificate application.
- All CA's are in the same secure physical location

8.1.2. Private Key delivery to subscriber

The private and public key pair generated by the Telstra Issuing CA's on behalf of an end user for the purpose of encryption (encryption certificate) will be delivered in a password protected PKCS #12 over a secure SSL session.

8.1.3. Public key delivery to certificate issuer

All Subscriber public-keys and certificates will be stored in the CA's repository and/or LDAP directory. Delivery of Subscribers public keys, from the Subscribers themselves or through an associated RA, shall be in PKCS #10 Certificate Signing Request (CSR) format. Public key delivery to the CA will be automatic and transparent to the subscriber.

8.1.4. CA public key delivery to relying parties

All Public keys and certificates will be stored in the CA's repository and/or LDAP directory. The Telstra Issuing CA public keys (as part of its certificate), and associated root certificate chain to the Telstra Issuing CA, shall be delivered to a Subscriber as part of the issuing process. The format will be PKCS #7 (binary or base64), with chain. The Telstra Issuing CA certificate has been delivered via AD Group policy, non domain members will have the chain delivered as part of the signing process in .p7b format, or can download the certificate from http://telstra-pki.pki.telstra.com.au/cps/

8.1.5. Key sizes

- The Telstra Issuing CA will use the RSA cryptography key algorithm with a minimum key length of 4096 bits.
- The Telstra Policy CA will use the RSA cryptography key algorithm with a minimum key length of 2048 bits.
- The Telstra issuing CAs will use the RSA cryptography key algorithm with a minimum key length of 2048 bits.
- The subscriber keys (end entities) will use the RSA cryptography key algorithm with a minimum key length of 2048 bits.
- Some exemptions may apply for applications not capable of 2048 bit key size, this will be at the discretion of the Telstra Issuing CA

8.1.6. Public key parameters generation and quality checking

8.1.6.1. CA key generation

Telstra CA Signature keys shall be generated using a random or pseudo-random

process as described in ISO 9564-1 and ISO 11568-5 that are capable of satisfying the statistical tests of FIPS 140-2 level 3. CA Keys are to be protected by a hardware cryptographic module rated at least FIPS 140-2 Level 3.

8.1.6.2. Subscriber key generation

Key pairs for end user Subscribers may be generated and stored in software or protected by secure cryptographic hardware module (e.g. smartcards, token) at the discretion of Telstra PKI PMA.

Application, device and Web Server Subscribers will generate its signing key pair using software or hardware key generation. In software the key pair generation will use the web server key generation tool / application (e.g., Microsoft Certificate Wizard, Apache tools). If hardware key generation is used (e.g., Crypto accelerator) the accelerator will be rated at FIPS 140-2 Level 2 or greater. Where possible, the web server SSL key pair will be generated on the web server that will be named in the DN of the certificate (as well as SubjectAltName).

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

See section 7 for key usage as per Section 9.1.1 base certificates and 9.1.2 certificate extensions.

- The Telstra CA signing keys are the only keys permitted to be used for signing certificates and CRLs. The certificate key usage field must be used in accordance with PKIX-1 certificate and CRL Profile. One of the following Key Usage values must be present in all certificates: Digital signature or non-repudiation. One of the following additional values must be present in CA certificate-signing certificates: Key Cert Sign, or CRL Sign.
- Application, device and web server SSL private key and certificate will only be used for web server authentication, VPN authentication and establishment of SSL sessions. The key usage will be set for digital signature and key encipherment. The extended key usage extensions, if used, will be restricted to 'Server Authentication'.

8.1.8. Hardware/Software Key generation

Key Generation Standards:

Confidentiality/Encryption Certificates Key pairs for all Entities may be generated in a software or hardware cryptographic module.

8.2. Private Key Protection and Cryptographic Module Engineering Controls

The certificate holder must protect its private keys from disclosure.

CA Keys are protected by a secure cryptographic hardware module rated at FIPS 140-2 Level 3 or higher.

The Subscriber is responsible for its private keys and shall protect its private key from disclosure according to the requirements as defined by this CPS and Telstra Corporation application and/or service requirements. Private Keys are only to be used for the intended purpose as defined by the certificate profile (section 7) and the subscriber agreement. At the time of creation of their private and public key pair, Subscribers are personally and solely responsible for the confidentiality and integrity of their private keys. Every usage of the private key is assumed to be the act of its owner.

The private key of a Subscriber shall be protected from unauthorized use by a combination of commercially reasonable cryptographic and physical access control mechanisms.

8.2.1. Cryptographic module standards and controls

The Telstra CA will utilize an HSM certified to FIPS 140-2 Level 3 to protect all CA private signing keys. Subscribers (Web servers) may either store the associated private signing

key in software (e.g., Microsoft registry), smartcard or in a SSL crypto accelerator, where applicable. The SSL crypto accelerator, if used, will be rated at FIPS 140-2 Level 2 or greater.

8.2.2. Private Key (m out of n) multi-person control

There is multiple person control for CA key generation operations. At a minimum, there is multi- person control for operational procedures such that no one person can gain control over the CA signing key. The principle of split knowledge and dual control as defined in section 7.2.2 shall be applied.

8.2.3. Private Key escrow

Private Key escrow is supported within the Telstra PKI for email and document encryption. End User encryption private keys will be recoverable through the use of the CA Key Recovery features; there will be no key escrow of end user authentication/digital signature private keys. There is multiple person control for key recovery operations.

There will be no key escrow of application server, device and web server SSL private keys.

8.2.4. Private Key backup

The Telstra Issuing CA will back up all CA private signing keys in a secure manner to support disaster recovery operations and as detailed in the Telstra Issuing CA Disaster Recovery Plan (DRP). Subscribers are responsible for backing up the private key associated with corporate application and/or service certificates in a secure manner (e.g., locked file cabinet, safe).

8.2.5. Private Key archival

The Telstra Issuing CA private signing key will not be archived.

8.2.6. Private Key transfer into or from a cryptographic module

If a Cryptographic module is used, the Private Key of the SCA is generated and retained in the module in an encrypted format. It will be decrypted only at the time at which it is being used. This access occurs over and encrypted network between the CA and the Luna HSM

8.2.7. Method of activating private key

The Private Keys of the Telstra Issuing CA and of SCAs are activated by Cryptographic software following the successful completion of a login process that validates an Authorised User to the HSM. The Entity must be authenticated to the cryptographic module before the activation of the private key. This authentication is in the form of tokens and a PIN entry device. Multiple person control is enforced on this process. When deactivated, private keys must be kept in encrypted form only.

8.2.8. Method of deactivating private key

The Security Profile for Telstra Corporation Limited PKI details which personnel are authorised to deactivate Private Keys and in what manner. This Document is not publicly available. When keys are deactivated they will be cleared from memory before the memory is de-allocated. Any disk space where keys were stored must be over-written before the space is released to the operating system. The cryptographic module automatically deactivates the private key after a pre-set period of inactivity.

8.2.9. Method of destroying private key

Please refer to Section 7.1.7 - Waste Disposal.

8.3. Other Aspects of Key Pair Management

8.3.1. Public key archival

The Telstra Issuing CA maintains a copy of all certificates issued within the CA database. The CA database is backed up and archived as part of CA operations. The Telstra Issuing CA shall retain all verification public keys for 7 years.

8.3.2. Certificate Operational Periods and Key Pair Usage Periods

The Telstra Issuing CA Key Pairs have the following usage periods:

- twenty five (25) years.

The Telstra Policy CA Key Pairs have the following usage periods:

- ten (10) years.

The Telstra issuing CA Key Pairs have the following usage periods:

- five (5) years.

The Telstra End-Entities Key Pairs have the following usage periods:

- no more than three (3) years.

8.4. Activation Data

8.4.1. Activation data generation and installation

All passwords used by the Telstra Issuing CA are in adherence to the Telstra Password complexity rules as defined in Telstra Corporation Corporate Directory.

8.4.2. Activation data protection

All pass phrases are known to current staff members of the Telstra Issuing CA. Change of staff will imply change of pass phrases. The Subscriber is responsible for its pass phrases and shall protect it from disclosure according to the requirements of Telstra Corporation application and/or service requirements.

8.4.3. Other aspects of activation data

No stipulation.

8.5. Computer Security Controls

8.5.1. Specific computer security technical requirements

The following functionality, for the Telstra Issuing CA, may be provided by the operating system, or through a combination of operating system, CA software, and/or physical safeguards (policies and procedures). Telstra CA server shall include the following functionality:

1. Access control to CA services and PKI roles,
2. Enforced separation of duties for PKI roles,
3. Identification and authentication of PKI roles and associated identities
4. Use of cryptography for session communication and database security, mutually authenticated and encrypted sessions are used for all external communications,
5. Archival of CA and end entity history and audit data,
6. Audit of security related events,
7. Trusted path for identification of PKI roles and associated identities, use of X.509 certificates for all CA administrators, and
8. Recovery mechanisms for keys and CA system.

8.5.2. Computer security rating

No stipulation

8.6. Life Cycle Security Controls

8.6.1. System development controls

Telstra Issuing CA uses CA software that has been designed and developed under a formal development methodology. An integrity verification process to influence security safeguard design and minimize residual risk should support the design and development process.

8.6.2. Security management controls

A formal configuration management methodology is used for installation and ongoing maintenance of Telstra Issuing CA. CA software, when first loaded shall provide a method for a Telstra Issuing CA to verify that the software on the system:

- Originated from the software developer;
- Has not been modified prior to installation; and
- Is the intended version.

The Telstra Issuing CA has commercially reasonable mechanisms and policies in place to control and monitor the configuration of the CA systems. All changes or modifications to the CA systems require approval by Telstra Corporation PKI PMA. The Telstra Issuing CA configuration management plan is detailed in the Telstra CA operating procedures.

8.6.3. Life cycle security ratings

No stipulation.

8.7. Network Security Controls

The Telstra Issuing CA server is protected by appropriate network security controls. Network security controls will permit only authorized access to the Telstra Issuing CA servers. Auditing will be enabled and checked on a frequent basis. Remote access to the Telstra Issuing CA environment will be protected by authenticated sessions. No other remote access is permitted to the host platform for system administration. All unnecessary services will be disabled, and the configuration will comply with Telstra Corporation most stringent standards for securing Windows Server hosts on the production network.

To protect the CA's networks, the appropriate network security controls are implemented. These controls include.

- Firewalls
- Intrusion detection systems
- Virus detection
- Integrity mechanisms to protect from modification
- Confidentiality mechanisms
- Access controls
- Mechanisms to prevent Denial of Service (DoS) attacks and hostile employee attacks.

The CA is on a secure network inside the secure facility. The Network is protected by a NIST compliant firewall(s). Access to the firewall is restricted to authorised personnel.

8.8. Time-stamping

No trusted time source is required for Telstra Issuing CA operations. The requirement for time- stamping of data is applicable to archives as described in section 5.

9. CERTIFICATE AND CRL PROFILES

9.1. Certificate Profile

9.1.1. Version number(s)

Telstra Issuing CA shall issue X.509 V3 certificates and X.509 v2 Certificate Revocation Lists (CRLs), in accordance with the PKIX Certificate and CRL Profile.

9.1.2. Certificate extensions

The Base Certificate Format will conform to the X.509 standard. The following represents the base certificate fields supported. Additional extensions are allowable if required. Every DN must be in the form of an X.501 printable String.

Certificate Field	Description
Version	3
Serial Number	Unique identifying number for this certificate assigned by the TELSTRA RSS CA
Signature	RSA with SHA-1
Issuer	Domain Name (DN) (X.500) of the issuing TELSTRA RSS CA
Validity	Start and expiry dates and times of the certificate
Subject	Domain Name (DN) (X.500) of the subject, as per Section 3.1.1 of this CPS
Subject public key information	The value of the public key for the subject along with an identifier of the algorithm with which this public key is to be used

9.1.2.1. CA Certificates

- The Telstra Issuing CA will support version 3 extensions in accordance with RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile’ dated April 2002.
- The Telstra CA certificate consists of the following extensions:

Field	Criticality	Description
Basic Constraint	Yes	Subject Type =CA; Path Length = 1
Authority Key Identifier	No	System Generated
Subject Key Identifier	No	System Generated
Certificate Policies	No	Identifies the Certificate Policy OID, URL and/or user notice; (PolicyIdentifier=1.3.6.1.4.1.1088.4.27.1.1.1)
CRL Distribution Point	No	Identifies how CRL information is published or Obtained URL and LDAP query.
Key Usage	Yes	Digital Signature, Certificate Signing, Off-line CRL

- Signing, CRL Signing
- The Telstra CA certificate consists of the following extensions:

Field	Criticality	Description
Basic Constraint	Yes	Subject Type =CA; Path Length = 0
Authority Key Identifier	No	System Generated
Subject Key Identifier	No	System Generated
Certificate Policies	No	Identifies the Certificate Policy OID, URL and/or user notice; **(PolicyIdentifier=1.3.6.1.4.1.1088.4.27.1.1.1)**
CRL Distribution Point	No	Identifies how CRL information is published or Obtained URL and LDAP query.
Key Usage	**Yes**	**Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing**
Certificate Template Name	No	SubCA

9.1.2.2. Application Server Certificates

- The Telstra Issuing CA will support the following extensions for SSL server certificates:

Field	Criticality	Description
Authority Key Identifier	No	System Generated
Subject Key Identifier	No	System Generated
Certificate Policies	No	Identifies the Certificate Policy OID, URL and/or user notice; (PolicyIdentifier=1.3.6.1.4.1.1088.4.27.1.1.1)
CRL Distribution Point	No	Identifies how CRL information is published or Obtained (URL and LDAP query).
Key Usage	No	Digital Signature; Key Encipherment
Extended Key Usage	No	Server Authentication; Client Authentication
Subject Alternative Name	No	SubjectAltName: dNSname = (optional)
Certificate Template Name	No	Telstra Live Comms Server

- The Telstra Issuing CA will support the following extensions for its End User Encryption certificates:

Field	Criticality	Description
Authority Key Identifier	No	System Generated
Subject Key Identifier	No	System Generated
Certificate Policies	No	Identifies the Certificate Policy OID, URL and/or user notice; (PolicyIdentifier=1.3.6.1.4.1.1088.4.27.1.1.1)
CRL Distribution Point	No	Identifies how CRL information is published or Obtained (URL and LDAP query).
Key Usage	No	Key Encipherment
Extended Key Usage	No	Secure Email
Authority Information Access	No	Identifies where to access CA information and Services (URL).
Subject Alternative Name	No	SubjectAltName: Principal Name =; RFC822 Name =;
Certificate Template Name	No	Telstra Email Encryption

9.1.3. Algorithm object identifiers

Telstra Issuing CA shall use and Subscribers shall support, for signing and verification, the following:

- RSA 2048 algorithm in accordance with PKCS#1; and/or
- SHA-2 or above algorithm in accordance with FIPS 180-4 and ANSI X9.30 part2; and/or
- Additional algorithms as supported by the CA software and implemented Hardware Security Module.

9.1.4. Name forms

Every DN must be in the form of an X.501 DirectoryString. Certificates issued by a CA contain the full X.500 distinguished name of the Certificate issuer and Certificate subject in the issuer name and subject name fields.

9.1.5. Name constraints

Subject and Issuer DNs must comply with PKIX standards and be present in all certificates.

9.1.6. Certificate policy object identifier

Certificate Policy extension will be used. The Object Identifier (OID) for this CPS will be set.

9.1.7. Usage of policy constraints extension

The Telstra Issuing CA supports the use of the Policy Constraints extension.

9.1.8. Policy qualifiers syntax and semantics

Telstra Issuing CA populates X.509 Version 3 certificates with a policy qualifier within the Certificate Policies extension. Generally, such certificates contain a CPS pointer qualifier that points to the applicable Telstra Issuing CA CPS. In addition, some Certificates contain a User Notice Qualifier which may point to an applicable relying party agreement.

9.1.9. Processing semantics for the critical certificate policy extension

The X.509 certificate profile complies with the Australian Standard X.509 profile. When applicable, critical extensions shall be interpreted as defined in PKIX.

9.2. CRL Profile

9.2.1. CRL checking requirements

All entity PKI software shall correctly process all CRL extensions required in the PKIX Part 1 Certificate and CRL Profile.

The Telstra Issuing CA will support and use the following CRL Version 2 extensions:

CRL Extension:

Field	Criticality	Description
Authority Key Identifier	No	Provides a means of identifying the CA's public key that corresponds to the private key used to sign the CRL.
CRL Number	No	CRL Number extension specifies a sequential number for each CRL issued by the CA.
Next CRL Publish	No	Next scheduled time/date that CRL will be published
Published CRL location	No	Location where CRL will be published to and can be retrieved

CRL Entry Extension:

Field	Criticality	Description
Reason Code	No	Identifies the reason for the certificate revocation; extension omitted if reason code is unknown.
Invalidity date	No	Date entry extension provides the date on which it is suspected that the private key was compromised.

9.3. OCSP profile

9.3.1. Version number(s)

No stipulation.

9.3.2. OCSP extensions

No stipulation.

9.3.3. On-Line revocation/status checking availability

As an alternative to CRL-checking, an on-line revocation-checking transaction to a trusted server, if available, may be used in accordance with the On-line Certificate Status Protocol (OCSP) as defined in the IETF X.509 Internet Public Key Infrastructure Online Certificate Status Protocol. Whenever an on-line Certificate status database is used as an alternative to a CRL, such database shall be updated immediately after revocation or suspension.

9.3.4. On-Line revocation/status checking requirements

Where on-line revocation/status checking is available and used by Relying Parties as an alternative to CRL checking, a Relying Party must check the status of all certificates in the certificate validation chain prior to their use. A Relying Party must also verify the authenticity and integrity of certificate status check responses received from an OCSP responder.

9.3.5. Other forms of revocation advertisements available

No stipulation

10. COMPLIANCE AUDIT AND OTHER ASSESSMENT

The Telstra Corporation Limited PMA will authorise audits for compliance where necessary. A compliance audit determines whether a CA's performance meets the standards established in this CPS. Telstra PKI Policy Management Authority shall outline specific requirements for a compliance audit. These requirements will conform to any statutory or regulatory requirements of the Commonwealth of Australia.

A Compliance Audit provides an independent third-party attestation that the Telstra Issuing CA is operating as stated in this CPS. The detailed information for the compliance audit is out of scope for this CPS.

11. OTHER BUSINESS AND LEGAL MATTERS

The detailed information for the compliance audit is out of scope for this CPS.

12. APPENDIX PKI DOCUMENTATION

The Telstra Corporation Limited PKI uses the following documents and websites for the provision of information to Relying Parties and Subscribers.

- Telstra PKI CA CPS
- Subscriber Application and Terms and Conditions document
- The Telstra PKI privacy policy

13. DEFINITIONS

13.1. Table of Acronyms and definitions

The following words, acronyms and abbreviations are referred to in this document.

Term	Definition
AD	Active Directory
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished name
DSA	Digital Signature algorithm
EDN	Enterprise Data Network
EAL	Evaluation assurance Level
EOI	Evidence of Identity ()
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ITU	International Telecommunications union
ISA	Information Security Authority
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
OCSP	On-line Certificate Status Protocol
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RCA	Root Certificate Authority
RFC	Request For Comment
RSA	Rivest-Shamir-Adleman
SHA –1	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SCA	Subordinate Certificate Authority
SSL	Secure Sockets Layer
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WIN2k3	Windows 2003 Server

14. GLOSSARY

A

Access Control
DEFINITION: The granting or denial of use or entry.

Activation Data
DEFINITION: Activation data, in the context of certificate enrolment, consists of a one-time secret communicated to the enrolling user (Subscriber) out of band. This shared secret permits the user to complete of the enrolment process.

Administrator
DEFINITION: A Trusted Person within the organization of a Processing Centre, Service Centre, Managed PKI Customer, or Gateway Customer that performs validation and other CA or RA functions.

Administrator Certificate
DEFINITION: A Certificate issued to an Administrator that may only be used to perform CA or RA functions.

Affiliated Individual
DEFINITION: An Individual having an affiliation with an Organization who has been authorized by the Organization to obtain a Certificate that identifies the Organization and the fact of the Individual's affiliation with the Organization. See "Sponsoring Organization."

Agent
DEFINITION: A person, contractor, service provider, etc. that is providing a service to Telstra under contract and are subject to the same corporate policies as if they were an employee of Telstra.

Applicant
DEFINITION: An Individual or Organization that submits application information to an RA or an Issuing CA for the purpose of obtaining or renewing a Certificate. See "Subscriber".

Application Server
DEFINITION: An application service that is provided to Telstra or one of its collaborative partners and may own a certificate issued under the TELSTRA RSS CA. Examples are Web SSL servers, VPN servers (IPSec), object signer services, Domain Controllers, etc.

Authentication
DEFINITION: the act of verifying. In the case of identities, the assurance of an identity.

Authority Revocation List (ARL)
DEFINITION: A list of revoked CA Certificates. An ARL is a CRL for CA Certificates.

Authorization
DEFINITION: The granting of permissions of use.

B

Business Process
DEFINITION: A set of one or more linked procedures or activities which collectively realize a business objective or policy goal, normally within the context of an organizational structure defining functional roles and relationships.

C

Certificate
DEFINITION: The public key of a user, together with related information, digitally signed with the private key of the Certification Authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509.

Certification Authority (CA)
DEFINITION: An authority trusted by one or more users to manage X.509 certificates and CRLs.

CA (Certification Authority) Room / Facility
DEFINITION: The room or facility where the CA systems and components are enclosed, and which the Telstra PKI Policy Authority has control regarding who has access to this room or facility.

Certification Chain

DEFINITION: An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.

Certificate Policy (CP)
DEFINITION: Named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. It is the principal statement of certificate policy governing the TELSTRA RSS CA. The CP is a high-level document that describes the requirements, terms and conditions, and policy for issuing, utilizing and managing certificates issued by a CA.

Certification Practice Statement (CPS)
DEFINITION: A statement of the practices, which a Certification Authority employs in issuing certificates. It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management and will be more detailed than the certificate policies supported by the CA.

Certificate Revocation List (CRL)
DEFINITION: A periodically issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation. CRL can be used to check the status of certificates.

Common Criteria
DEFINITION: The Common Criteria is an Internal agreed upon IT Security evaluation criteria. It represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community.

Confidential
DEFINITION: A security classification used to describe information which if disclosed could result in personal loss or minor financial loss. Personal information and tactical information would be deemed confidential.

Confidentiality
DEFINITION: Information that has an identifiable value associated with it such that if disclosed might cause damage to an entity.

Cross Certification
DEFINITION: The process describing the establishing of trust between two or more CAs. Usually involves the exchange and signing of CA certificates and involves the verification of assurance levels.

D

Distinguished Encoding Rules (DER)
DEFINITION: The Distinguished Encoding Rules for ASN.1, abbreviated DER, gives exactly one way to represent any ASN.1 value as an octet string. DER is intended for applications in which a unique octet string encoding is needed, as is the case when a digital signature is computed on an ASN.1 value.

Digital Signature
DEFINITION: The result of the transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine that the key that corresponds to the signer's key created the transformation and the message was not altered.

Distinguished Name (DN)
DEFINITION: Every entry in a X.500 or LDAP directory has a Distinguished Name, or DN. It is a unique entry identifier throughout the complete directory. No two Entries can have the same DN within the same directory. A DN is used in certificates to uniquely identify a certificate-owner. Example of a DN:
cn=Road Runner, ou=bird, dc=carton, dc=com
ou=bird, dc=carton, dc=com
dc=carton,
dc=com dc=com

Dual Control
DEFINITION: A process utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information, whereby no single entity is able to access or utilize the materials, e.g., cryptographic key.

E

E-mail Certificates
DEFINITION: Certificates utilized for encrypting and verifying digital signatures. Normally two separate certificate: one for encryption, the other for signature verification.

Entity
DEFINITION: Any autonomous element or component within the Public Key Infrastructure that participate is one form or another, such managing certificates or utilizing certificates. An Entity can be a CA, RA, Subscriber, Relying Party, etc.

F

FIPS 140-2
DEFINITION: Federal Information Processing Standard 140-2(FIPS 140-2) is a standard that describes US Federal government requirements that IT products shall meet for Sensitive, but Unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST), has been adopted by the Canadian government's Communication Security Establishment (CSE), and is likely to be adopted by the financial community through the American National Standards Institute (ANSI). The different levels (1 to 4) within the standard provide different levels of security and in the higher levels have different documentation requirements.

FIPS 180-1
DEFINITION: Standard specifying a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data files.

G

H

Hardware Security Module
DEFINITION: Hardware used to perform cryptographic functions and store cryptographic keys in a secure fashion. HSMs are FIPS rated to level 1 through 4, with 4 being the most secure.

I

Identification and Authentication (I&A)
DEFINITION: To ascertain and confirm through appropriate inquiry and investigation the identity of an End Entity or Sponsoring Organization.

Integrity
DEFINITION: ensuring consistency of an object or information. Within security systems, integrity is the principle of ensuring that a piece of data has not been modified maliciously or accidentally.

ISO 9564-1
DEFINITION: Basic principles and requirements for online PIN handling in ATM and POS systems, provides instructions to financial institutions in the development, implementation and/or the operation of systems and procedures for the protection of PIN throughout its lifecycle.

ISO 11568-5
DEFINITION: Basic principles and requirements for Key lifecycle for public key cryptosystems, provides instructions to financial institutions in the development, implementation and/or the operation of systems and procedures throughout Key’s lifecycle

J

K

Key
DEFINITION: When used in the context of cryptography, it is a secret value, a sequence of characters that is used to encrypt and decrypt data. A key is a unique, generated electronic string of bits used for encrypting, decrypting, e-signing or validating digital signatures.

Key Pair
DEFINITION: Often referred to as public/private key pair. One key is used for encrypting and the other key used for decrypting. Although related, the keys are sufficiently different that knowing one does not allow derivation or computation of the other. This means that one key can be made publicly available without reducing security, provided the other key remains private.

L

Lightweight Directory Access Protocol
DEFINITION: LDAP is the standard Internet protocol for accessing directory servers over a network.

M

MD5
DEFINITION: One of the message digest algorithms developed by RSA Security Inc.

N

Non-repudiation
DEFINITION: protection against the denial of the transaction or service or activity occurrence.

O

Object Identifier (OID)
DEFINITION: The unique alpha-numeric identifier registered under the ISO registration standard to reference a standard object or class.

P

Personal information
DEFINITION: Information about a person or individual and having the meaning given to that term in the Privacy Act 1988 (Cth).

PKCS #1
DEFINITION: Standard that provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptographic primitives; encryption schemes; signature schemes, etc.

PKCS #7
DEFINITION: A cryptographic message format or syntax managed and edited by RSA Laboratories. A standard describing general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.

PKCS #10
DEFINITION: A certificate request format or syntax managed and edited by RSA Laboratories. It is a standard describing syntax for a request for certification of a public key, a name, and possibly a set of attributes.

Public Key Infrastructure (PKI)
DEFINITION: The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based Public Key Cryptography system. A set of policies, procedures, technology, audit and control mechanisms used for the purpose of managing certificates and keys.

PKIX
DEFINITION: The Public Key Infrastructure (X.509) or PKIX is an IETF Working Group established with the intent of developing Internet standards needed to support an X.509-based PKI. The scope of PKIX extends to also develop new standards for use of X.509-based PKIs in the Internet.

PKI Personnel
DEFINITION: Persons, generally employees, associated with the operation, administration and management of a CA or RA.

Policy
DEFINITION: The set of laws, rules and practices that regulates how an organization manages its business. Specifically, security policy would be the set of laws, rules and practices that regulates how an organization manages, protects and distributes sensitive information.

Policy Management Authority (PMA)
DEFINITION: This forum is to replace the PKI Governance Council and the role is owned by the APAC CISO in line with current cyber governance approaches and frameworks

Printable String
DEFINITION: String format for representing names, such as Common Name (CN), in X.509 certificates. The encoding of a value in this syntax is the string value itself.

Private Key
DEFINITION: The private key is one of the keys in a public/private key pair. This is the key that is kept

secret as opposed to the other key that is publicly available. Private keys a utilized for digitally signing documents, uniquely authenticating an individual, or decrypting data that was encrypted with the corresponding public key.

Public Key Infrastructure
DEFINITION:

Public

DEFINITION: A security classification for information that if disclosed would not result in any personal damage or financial loss.

Public Key
DEFINITION: The community verification key for digital signature and the community encryption key for encrypting information to a specific Subscriber.

PKI Policy Management Authority
The role is owned by the APAC CISO in line with current cyber governance approaches and frameworks

Q

R

Registration Authority (RA)
DEFINITION: An entity that performs registration services on behalf of a CA. RAs work with a particular CA to vet requests for certificates that will them be issued by the CA.

Rekey
DEFINITION: the process of replacing or updating the key(s). The expiration of the crypto period involves the replacement of the public key in the certificate and therefore the generation of a new certificate. TELSTRA ISSUING CA does not support rekey.

Relative Distinguished Name (RDN)
DEFINITION: A Distinguished Name is made up of a sequence of Relative Distinguished Names, or RDNs. The sequences of RDNs are separated by commas (,) or semi-colons (;). There can be more than one identical RDN in a directory, but they must be in different bases, or branches, of the directory. Example of a DN is “cn=Road Runner,ou=bird,dc=carton,dc=com”
RDNs would be:
RDN => cn=Road Runner
RDN => ou=bird
RDN => dc=carton
RDN => dc=com

Relying Party
DEFINITION: An entity that uses a certificate signed by the CA to authenticate a digital signature or encrypt communications to a subject. The relying party relies on the certificate and normally is but does not have to be a Subscriber of the PKI. In the context of TTE, A relying party is a Telstra user that rely on the Telstra device’s digital certificate to trust that Telstra service, i.e, Service receiver.

Repository
DEFINITION: A place or container where objects are stored. A data repository is technology where data is stored logically. In PKI terms, a repository accepts certificates and CRLs form one or more CAs and makes them available to entities that need them for implementing security services.

Revocation
DEFINITION: In PKI, revocation is the action associated with revoking a certificate. Revoking a certificate is to make the certificate invalid before its normal expiration. The Certification Authority that issued the certificate is the entity that revokes a certificate. The revoked status is normally published on a certificate revocation list (CRL).

RSA
DEFINITION: A public key cryptographic algorithm invented by Rivest, Shamir, and Adelman..

S

Secure Hash Algorithm (SHA-1)
DEFINITION: An algorithm developed by the U.S. National Institute of Standards & Technology (N IST). SHA-1 is used to create a cryptographic hash (or “fingerprint”) of a message or data.

Secure Sockets Layer (SSL)
DEFINITION: SSL is a protocol layer created by Netscape to manage the security of message transmissions in a network. Security is achieved via encryption. The “sockets” part of the term refers to the sockets method of passing data back and forth between client and server programs in a network or between program layers in the same computer.

Sensitive
DEFINITION: Used to describe the security classification of information where the information if disclosed would result in serious financial loss, serious loss in confidence or could result in personal harm or death.

Signature Verification Certificate

DEFINITION: Often referred to as simply a Signature Certificate. It is the certificate containing the public key used to verify a digital signature that was signed by the corresponding private key.

Split Knowledge
DEFINITION: a condition under which two or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key. The resultant key exists only within secure cryptographic devices

SSL Client Certificate
DEFINITION: Certificate utilized to verify the authentication of an end user to a server when a connection is being established via a SSL session (secure channel)..

SSL Server Certificate
DEFINITION: Certificate utilized to verify the authentication of a web or application server to the end user (client) when a connection is being established via a SSL session (secure channel).

Subscriber
DEFINITION: A Subscriber is an entity; a person or application server that is a holder of a private key corresponding to a public, and has been issued a certificate. In the case of an application server, a person authorized by the organization owning the application server may be referred to as the Subscriber. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the certificate.

Surveillance Camera
DEFINITION: A surveillance camera is a video recording device used for detection and identification of unauthorized physical entry to a secured area. A camera used for recording a signing ceremony for auditing purposes is not considered a surveillance camera.

T

Threat
DEFINITION: a danger to an asset in terms of that asset's confidentiality, integrity, availability or legitimate use.

TERM: Token
DEFINITION: Hardware devices normally associated with a reader, used to store and/or generate encryption keys, such as smartcards and USB tokens.

U

URI
DEFINITION: Universal Resource Indicator - an address on the Internet.

UTF8String
DEFINITION: UTF-8 is a type of Unicode, which is a character, set supported across many commonly used software applications and operating systems. UTF-8 is a multibyte encoding in which each character can be encoded in as little as one byte and as many as four bytes. Most Western European languages require less than two bytes per character. Greek, Arabic, Hebrew, and Russian require an average of 1.7 bytes. Japanese, Korean, and Chinese typically require three bytes per character. Such Unicode is important to ensure universal character / foreign characters are supported.

V

Valid Business Relationship
DEFINITION: A relationship between Telstra and an Telstra's partner, supplier, member or other business affiliation, or an agent representing an Telstra's partner, supplier, member or other business affiliation, or an approved contractor; and a have a requirement to access Telstra's electronic services. An Electronic Access Agreement will be in place with the organization representing this relationship.

RA administrator
DEFINITION: A person who verifies information provided by a person applying for a certificate.

Vulnerability
DEFINITION: weaknesses in a safeguard or the absence of a safeguard.

W

WebTrust
DEFINITION: A described framework for Certificate Authorities to assess the adequacy and effectiveness of controls employed by Certificate Authorities. See WebTrust Principles and Criteria for Certificate Authorities at http://www.webtrust.org.

X

X.500
DEFINITION: Specification of the directory service required to support X.400 e-mail initially but common used by other applications as well.

X501 PrintableString
DEFINITION: String format for representing names, such as Common Name (CN), in X.509 certificates. The encoding of a value in this syntax is the string value itself; an arbitrary string of printable characters.

X.509
DEFINITION: An ISO standard that describes the basic format for digital certificates.

X.509 v3 Certificate Extension
DEFINITION: Generally CA software supports X.509 v3 certificate extensions, including extensions for PKIX, S/MME, and SSL certificates. These extensions conform to version 3 of the X.509 standard, as stated in RFC 3280 'Internet X.509 Public Key Infrastructure Certificate and CRL Profile' dated April 2002 and specify additional constraints or capabilities on the certificate subject.

Y

Z

15. APPENDIX ARCHIVES ACT 1983

http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/all/search/FFAF1E0B63963261CA2572480026151A

The Archives Act 1983 sets out comprehensive arrangements for dealing with Commonwealth records and establishes the Australian Archives as an organisation. The Archives Act sets out basic principles to ensure record keeping is both efficient and accountable, and describes actions which must be taken by Commonwealth agencies to retain, destroy, store or otherwise deal with records. As well as encouraging efficiency for the short term, the Act places a wider responsibility on government agencies to protect records, especially those of a long term or permanent value, which must be preserved for future access by the agency, the Government and members of the public.

The Act describes the functions of Australian Archives and its roles and responsibilities:

- it defines Australian Archives' role in the preservation and management of the Commonwealth's records;
- it establishes the fundamental right of public access to Commonwealth records
- over 30 years old;
- it defines the responsibilities of the Commonwealth with regard to record
- retention, noting that records may only be destroyed :
- as required by law
- in accordance with current Australian Archives' approved Disposal Authorities
- in accordance with a normal administrative practices approved by the Australian Archives; and
- it requires Archives to encourage and facilitate the use of the archival resources of the Commonwealth.
- The Archives Act 1983 imposes statutory obligations on all government departments for the management of their records. the Act empowers the Australian Archives to control the disposal of Commonwealth records to ensure:
- efficient and economical record keeping in he Commonwealth Government by the prompt destruction of records no longer needed for legal, fiscal, administrative or other reasons; and
- identification and preservation of those records which for similar reasons must be kept permanently.
- Strict controls are imposed on the management of Commonwealth records throughout their life cycle. Under the Act it is illegal to destroy or otherwise dispose of a record, to transfer custody or ownership of a record or to damage or alter a record unless these actions are:
- required by law;
- authorised by the Australian Archives; or
- a normal administrative practice.

The Act permits normal administrative practices involving disposal, alteration or transfer of Commonwealth records, as long as these do not undermine the proper preservation of Commonwealth records or endanger valuable information.

2006 Amendment

http://www.aph.gov.au/library/pubs/bd/2006-07/07bd058.htm.

16. OTHER POLICY

Document	Version /Date	Status
Telstra Physical Security Standard	V8.0 | Feb.2020	Current

NIST - FIPS References

Series	Number	Title	Status	Release Date
FIPS	205	Stateless Hash-Based Digital Signature Standard	Draft	8/24/2023
FIPS	204	Module-Lattice-Based Digital Signature Standard	Draft	8/24/2023
FIPS	203	Module-Lattice-Based Key-Encapsulation Mechanism Standard	Draft	8/24/2023
FIPS	202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	Final	8/04/2015
FIPS	201-3	Personal Identity Verification (PIV) of Federal Employees and Contractors	Final	1/24/2022
FIPS	200	Minimum Security Requirements for Federal Information and Information Systems	Final	3/01/2006
FIPS	199	Standards for Security Categorization of Federal Information and Information Systems	Final	2/01/2004
FIPS	198-1	The Keyed-Hash Message Authentication Code (HMAC)	Final	7/16/2008
FIPS	197	Advanced Encryption Standard (AES)	Final	5/09/2023
FIPS	186-5	Digital Signature Standard (DSS)	Final	2/03/2023
FIPS	180-4	Secure Hash Standard (SHS)	Final	8/04/2015
FIPS	140-3	Security Requirements for Cryptographic Modules	Final	3/22/2019
FIPS	140-2	Security Requirements for Cryptographic Modules	Final	12/03/2002