Policy Document

Telstra Root CA

Certificate Practices statement

Published By: Telstra Corporation Ltd

Author:
Paul Lexa

PKI Specialist

Telstra Corporation Limited
ABN 33 - 051 775 556

Trademark Notices

TABLE OF CONTENTS

1. PURPOSE

In order to support the secure movement of Telstra Corporation Limited information within or across Networks and Partner Company boundaries, it is necessary to authenticate and verify subscribers of the public key infrastructure in the Telstra Corporation Limited environment. Telstra Corporation Limited communications generally involve the transfer of highly commercially sensitive information. Moving to a digitally signed and/or encrypted environment for these communications therefore demands a high degree of confidence that the information will be transferred securely and that the integrity of the parties is not in dispute.

This document is intended to provide information surrounding the security of the Telstra PKI implementation, including both physical and Logical

In a Public Key Infrastructure, a Certification Authority acts as a trusted party to facilitate the confirmation of the relationship between a public key and a named entity. The Certification Authority issues digital certificates that can be used for authentication, authorisation, encryption and digital signatures. The certification authority also performs certificate management services such as publication and revocation of digital certificates. As Certification Authorities play a vital role in facilitating secure electronic transactions, there needs to be assurance that the Certification Authorities perform their roles and duties with high levels of integrity and security. This document presents the requirements, which forms the basis for the operation of a Certification Authority in the Telstra Corporation Limited environment and serves as guidelines or criteria in the cross-certification process with other Certification Authorities (Initially Partner companies, one day potentially as a Commercial trusted PKI). However, the document may require further consideration of many points to cover the future development of related technologies such as encryption algorithms, key length and new features in an application, to name a few. 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 certification authorities.

Importantly, this document does not aim to provide legal advice or recommendations.

2. SCOPE

The scope of this document is limited to discussion of the topics that can be covered in a CPS as defined in the Digital Signature Guidelines (DSG) and PKI Assessment Guidelines (PAG). In particular, this document describes the types of information that should be considered for inclusion in a CPS. While this information generally assumes use of the X.509 version 3 certificate format, for the purpose of providing assurances of identity, it is not intended that the material be restricted to use of that certificate format or identity certificates. Rather, it is intended that this framework be adaptable to other certificate formats and to certificates providing assurances other than identity that may come into use. The scope extends to defining security policies, and provides information surrounding the security of the Telstra PKI implementation, including both physical and Logical. Essentially, in presenting this framework, this document should be viewed and used as a flexible tool, presenting topics that should be considered of particular relevance to this CPS. This document assumes that the reader is familiar with the general concepts of digital signatures, certificates, and public-key infrastructure (PKI), as used in X.509, the DSG, and the PAG.

3. INTRODUCTION

This document is the Telstra Root CA Certification Practice Statement ("CPS"). It is a statement of the practices that the Telstra Root CA employs in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with specific requirements.

This CPS is specifically applicable to:

- Telstra Corporation Limited's Internal Root Certification Authority.

- Telstra Corporation Limited Infrastructure CAs, and Telstra Corporation limited administrative CAs supporting the Telstra Corporation Limited " Telstra Trust Environment"

More generally, the CPS also governs the use of Telstra Root CA services within Telstra Corporation Limited's TTE by all individuals and entities within Telstra Corporation Limited's Trust Environment (collectively, Telstra Corporation Trust Environment Participants"). The CPS is a single document that defines these certificate policies, one for each of the Classes, and sets TTE Standards for each Class.

Telstra Corporation Limited currently offers three Classes of Certificates within its Sub domain of the TTE. This CPS describes how Telstra Corporation Limited meets the CP requirements for each Class within its Telstra Trust Environment. Thus, the CPS, as a single document, covers practices and procedures concerning the issuance and management of all three Certificate Classes. Telstra Corporation Limited 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. The CPS is only one of a set of documents relevant to Telstra Corporation Limited's Trust Environment. These other documents include:

Ancillary confidential security and operational documents that supplement the CP and CPS by providing more detailed requirements, such as:

- The Telstra Corporation Limited Physical Security Policy, which sets forth security principles governing the TTE infrastructure,
- The Telstra Corporation Limited 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 Corporation Limited. These agreements bind Customers, Subscribers, and Relying Parties of Telstra Corporation Limited. 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. In many instances, the CPS refers to these ancillary documents for specific, detailed practices for implementing TTE Standards, where including the specifics in the CPS could compromise the security of Telstra Corporation Limited's TTE.

The commencement date of the Telstra Corporation Limited Root Certification Authority Certification Practice Statement (Telstra Corporation Limited RCA CPS) is the date the Telstra Root CA generates, it's self signed certificate.

The commencement date of this CPS is: **17 December 2009**

Telstra Corporation Limited has authority over the Telstra Trust Environment. This environment includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties.

The CPS sets forth the business, legal and technical practices and procedures for approving, managing, revoking and renewing digital certificates within the Telstra Corporation Limited's trust environment. More specifically, this CPS provides the context under which certificates are requested, created, issued, renewed, and/or used by Subscribers, it describes the practices that Telstra Corporation Limited employs for:

- Securely managing the core infrastructure that supports the TTE, and

- Issuing, managing, revoking, and renewing TTE Certificates within Telstra Corporation Limited's Sub domain of the TTE, in accordance with the requirements of the CPS and its TTE Standards.

This CPS conforms to the Internet Engineering Task Force (IETF) PKIX Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework (also known as RFC 3647).

This CPS does not provide details on the operations of the Telstra Root CA; rather it provides the overview of the practices, and outlines the rules applying to and scope of use of Telstra Corporation Limited PKI Certificates.

Details of the operations are found in supporting documents, such as Telstra Corporation PKI Operating Procedures.

This document uses several technical concepts associated with PKI technology. To become familiar with the terminology used, we strongly recommend that you read the Definitions and Acronyms appendices before reading the document and refer to it as needed while reading the CPS content. The security mechanisms provided by the Telstra Corporation Limited PKI are intended for use in combination with one or more additional security conventions to give protection appropriate to sensitive information.

This document content is divided into nine sections:

- Section 3 – provides an overview of the policy 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, and 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 with regard to 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 – addresses topics covered and methodology used for assessments/audits; frequency of compliance audits or assessments; identity and/or qualifications of the personnel performing the audit or assessment; actions taken as a result of deficiencies found during the assessment; and who is entitled to see results of an assessment.
- Section 11 – covers general business and legal matters: the business issues of fees, liabilities, obligations, legal requirements, governing laws, processes, confidentiality, etc.

3.1. Overview

3.1.1. General

In general, a public-key certificate (hereinafter "certificate") binds a public key held by an entity (such as a person, organization, account, device, or site) to a set of information that identifies the entity, associated with use of the corresponding private key. In most cases involving identity certificates, this entity is known as the "subject" or "subscriber" of the certificate. Two exceptions,

however, include devices (in which the subscriber is usually the individual or organization controlling the device) and anonymous certificates (in which the identity of the individual or organization is not available from the certificate itself).

A certificate is used by a "certificate user" or "relying party" that needs to use, and rely upon the accuracy of the binding between the subject public key, distributed via that certificate and the identity and/or other attributes of the subject contained in that certificate.

A relying party is frequently;

- an entity that verifies a digital signature from the certificate's subject where the digital signature is associated with an email, web form, electronic document, or other data.

Other examples of relying parties can include;

- a sender of encrypted email to the subscriber,
- a user of a web browser relying on a server certificate during a secure sockets layer (SSL) session, an entity operating a server that controls access to online information using client certificates as an access control mechanism.
- In summary, a relying party is an entity that uses a public key in a certificate (for signature verification and/or encryption).

The degree to which a relying party can trust the binding embodied in a certificate depends on several factors. These factors can include the practices followed by the certification authority (CA) in authenticating 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).

A Version 3 X.509 certificate may contain a field declaring that one or more specific certificate policies apply to that certificate. According to X.509, a certificate policy (CP) is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements."

In general, a PKI consists of a hierarchy of Trusted Elements and Subscribers. In the Telstra Corporation Limited Enterprise PKI, the hierarchy of Trusted Elements comprises the Telstra Root CA (Telstra Corporation Limited RCA), Telstra Policy CA1, Enterprise Subordinate CA's (Telstra AD Objects CA1, Telstra User Issuing CA1), Extended Services Registration Authorities (Registration Authority or RA), and End User or Subscribers.

The Telstra Corporation Limited PKI is designed and operated to comply with the broad strategic direction of existing international standards for the establishment and operations of a PKI.

The Telstra Corporation Limited PKI supports the creation and use of key pairs and of Public Key Certificates. Key pairs and Public Key Certificates are used in the provision of Telstra Corporation Limited PKI certificate services that include but are not limited to:

- Authentication services (authentication, integrity and non-repudiation) and
- Confidentiality services.
- Encryption Services

3.1.2. Certificate Policy Document

This CPS covers the requirements of individual CP's

3.1.3. Policy overview

The Policy Object Identifier Designation for this CPS is (OID = 1.3.6.1.4.1.1088.4.27.1.1.1)

The policies are designed for use in certain situations, and identify specific roles and responsibilities for Certificate Authorities (CA) issuing certificates under the Telstra Corporation Limited PKI and for Registration Authorities (RAs), Subscribers and Relying Parties under the Telstra Corporation Limited PKI; all have specific obligations outlined in this policy.

The term "ESI" (Electronic Signature Infrastructure) might be useful to describe a particular framework established for a specific community or class of applications.

A CA must associate itself with and use one or more Certificate and one or more CRL repositories. Certificates must be made available to Subscribers.

The use of confidentiality/encryption keys is appropriate for the confidentiality/encryption of designated information.

The use of Certificate Policy Digital Signatures Medium Assurance is appropriate for all transactions that require authentication and / or a signature.

The use of Certificate Policy Digital Signatures High Assurance is appropriate for all transactions that require authentication and /or a signature that require a high-level of assurance.

Telstra Corporation Limited disclaims all liability for any use of a certificate issued by a CA in accordance with this policy and the Telstra Corporation Limited PKI. Any disputes concerning key or certificate management under this policy are to be brought in the courts of the Australia and governed by the statutes and laws Australia, without regard to conflicts of laws principles thereof. Certificates may be issued under this policy following authentication of a Subscriber's identity. Identification will be in the manner set out in this policy.

The Telstra Root CA will revoke certificates in the circumstances enumerated in this policy. The Telstra Root CA will maintain records or information logs in the manner described in this policy. The Telstra Root CA will ensure the separation of critical CA functions between at least three individuals assigned to distinct trusted roles.

Digital Signature private keys will not be exportable or escrowed in any form. Digital signature Keys have a validity period as indicated in this policy.

Confidentiality/Encryption private keys issued by The Telstra Root CA may be backed-up to protect against data loss or data corruption. Applications that require recoverable encrypted messaging will employ Confidentiality/Encryption framework, which defines confidentiality with key recovery for the encryption use.

Such applications may also use a Digital Signature framework, but only for a separate authentication signature and as long as there is no mingling of the two types of Certificates in a repository. Certificates based on the Digital Signature framework rely on the Subscriber's sole possession to assert the right of Non-Repudiation and must not be mingled with any Certificates that allow recovery and thereby break the criteria of sole possession. No information provided by a Subscriber to The Telstra Root CA shall be disclosed without the Subscriber's consent, unless required by law or court order. The Telstra Root CA activities are subject to inspection by the PKI Governance Council's (PGC) or its agents at the discretion of the PGC.

3.2. Document Name and Identification

This document is the Telstra Root CA Certification Practice Statement.

The Policy Object Identifier Designation for this CPS is registered under the Policy Management Authority. The OID for the Telstra Root CA Certificate Practices Statement (Telstra Root CA CPS) is OID = 1.3.6.1.4.1.1088.4.27.1.1.1

3.2.1. Common Elements

This Telstra Corporation Limited CPS covers the common practices and procedures that apply to the entire Telstra Corporation Limited PKI Hierarchies, as operated by Telstra Corporation Limited under control of the Telstra PKI Governance Council (PGC).

These common elements include:

- the use of Evaluated Products for any of the security-critical cryptographic operations;

- the separation of registration and certification operations, with registration operations generally being performed on a remote site managed and operated by the Telstra Corporation Limited PKI Operations;
- the application of tiered security comprising prevention, detection and considered response;
- the employment of trustworthy personnel who have been independently vetted to the HIGHLY PROTECTED security level;
- the 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 and external audits to ensure a high level of operational integrity is always maintained.

3.2.2. Relationship between the CPS and Certificate Policies

The full set of practices, procedures, terms and conditions relating to a particular Certificate can be determined by reading:

- Telstra Root CA CPS;

3.2.3. Certification Authority Certificate Practice Statement

This Telstra Corporation Limited Root Certification Authority Certificate Practice Statement (Telstra Root CA CPS) relates to:

- the self-signed Telstra Root CA authentication and confidentiality Certificates which the Telstra Root CA issues to itself; and
- The authentication and confidentiality Certificates signed by the Telstra Root CA and issued to Telstra Policy CA1.
- The authentication and confidentiality Certificates signed by the Telstra Policy CA1 and issued to Telstra Subordinate Certification Authorities.
- The Confidentiality/encryption, and digital signature certificates issued by issuing CA's to it's subscribers

3.2.4. Documentation

Telstra Corporation Limited conducts its Telstra Corporation Limited RCA role in accordance with the following public documents:

- Corporation Telstra Root CA CPS;
- Commercial-in-Confidence or HIGHLY PROTECTED documents which are not publicly available.

3.2.5. Telstra Certification Authority Certificate Practice Statement

Telstra Root CA CPS as Specified element under the Telstra Corporation Limited PKI has been assigned an X.500 Object Identifier (OID). The authority for issuing an OID is the Telstra Corporation Limited PKI Governance Council (Telstra Corporation Limited PGC).

The Telstra Corporation Limited RCA CPS is published at:
http://telstra-pki.pki.telstra.com.au/TelstraCPS.pdf

3.2.6. Obligations

3.2.6.1. CA Obligations

The Telstra Root 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, and for ensuring that all aspects of the CA Services and CA operations and infrastructure related to certificates issued under this CPS are performed in accordance with the requirements, representations, and warranties of this CPS.

The Telstra Root CA will operate in accordance with its CPS, and all applicable laws of the Commonwealth of Australia when fulfilling these obligations. The Telstra Root 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.

3.2.7. Representations by the Telstra Root CA

By issuing a certificate that references this CPS, the Telstra Root 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 and in accordance with this Policy, that:

- The Telstra Root CA has issued, and will manage, the certificate in accordance with this CPS, any applicable PGC regulations and any applicable state statute or regulations and that the certificate meets all material requirements of the Telstra Root CA's 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 policy that apply to them;
- Have in place mechanisms and procedures that include written agreements (Subscriber agreements and Relying Party agreements) as approved by the PGC to ensure that Subscribers and Relying Parties (collectively known as End- Entities) are aware of, and agree to abide with, the stipulations in this policy 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 the PKI;
- There are no misrepresentations of fact in the certificate known to the Telstra Root CA, and the Telstra Root 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
- Maintain a statement in compliance with identified Commonwealth of Australia statute reciting the Telstra Root CA 's statutory obligation to maintain the confidentiality of personal information in accordance with the provisions of such statute.

3.2.8. Notification of certificate issuance and revocation

Telstra Corporation Issuing CA's will make CRLs available to Subscriber's or Relying Parties in accordance with this CPS, Telstra Corporation Issuing CA's will notify a Subscriber when a certificate bearing the Subscriber's DN is issued, suspended, reinstated, or revoked.

3.2.9. Accuracy of representations

When an Issuing CA publishes a certificate it certifies that it has issued a certificate to a Subscriber and that 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 Root 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 PGC. Such agreements will include, 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 Root 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 Root 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.

3.2.10. 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. The Telstra Issuing CA's will provide a process that ensures that the period for which the Telstra Root CA has to complete its initialization process is no longer than three working days.

3.2.11. Certificate revocation and Renewal

The Telstra Issuing 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 the Subscriber Agreement and any other applicable document outlining the terms and conditions of the certificate use. The Issuing CA must ensure that the key changeover procedures are in accordance with 6.3 and 6.4. The Issuing 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.

3.2.12. Revocation Request

The Telstra Root CA, or RA acting on its behalf, must authenticate a request for revocation of a certificate. The Telstra Root 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.

3.2.12.1. Circumstances for revocation

A Subscriber may request revocation of their individual Certificate at any time for any reason. A sponsoring organization may, where applicable, request revocation of an affiliated individual Certificate at any time for any reason. The issuing CA may also revoke a Certificate upon failure of the Subscriber (or any sponsoring organization, where applicable) to meet its obligations under this CPS, or any other agreement, regulation, or law 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. The PGC may, at its discretion, revoke a cross-certificate when a CA fails to comply with obligations set out in this CPS, or any agreement, or any applicable law.

A certificate must be revoked:

- when any of the information in the certificate changes;
- upon suspected or known compromise of the private key;
- Upon suspected or known compromise of the media holding the private key.

3.2.12.2. 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 organization that made the application for the certificate on behalf of device or application;
- the Sponsor whenever an affiliated individual is no longer affiliated with the Sponsor;
- 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;

The revocation of a cross-certificate may only be requested by:

- The CA on whose behalf the cross-certificate was issued;
- The PGC. In the event that the CA ceases operations, all Certificates issued by the CA shall be revoked prior to the date that the CA ceases operations.

3.2.12.3. Procedure for revocation request

The Telstra Root 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 Root 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. A revocation request that is submitted electronically with a digital signature based on the old private key is considered authenticated upon receipt.

3.2.12.4. Revocation Request grace period

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 Root CA or within the following:

- Confidentiality/Encryption Certificate Twenty-four (24) hours of receipt Digital Signature Medium Assurance Certificate Twelve (12) hours of receipt Digital Signature
- High Assurance Certificate Initiated immediately upon receipt

3.2.12.5. Circumstances for Certificate suspension (or hold)

If the Telstra Root CA or RA receives notification from a Subscriber or Sponsor 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 Root CA or RA, the Telstra Root 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.

3.2.12.6. Who can request Suspension

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

3.2.12.7. Procedure for suspension request

The procedures for issuing a certificate suspension request are published in the Telstra Root CA's CPS.

The Telstra Root 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.

3.2.12.8. Limits on suspension period

The suspension period may not exceed 5 working days.

3.2.12.9. Protection of private keys

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

3.2.12.10. 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's 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.

3.2.12.11. Repository Obligations

Certificates and CRLs are available to Relying Parties in accordance section 4.1

3.2.12.12. Registration Authorities (RA)

The Telstra Root CA shall be responsible for performing all identification and authentication functions and all certificate manufacturing and issuing functions. However, the Telstra Root CA may delegate these functions to an identified Registration Authority (RA) provided that the Telstra Root CA remains primarily responsible for the performance of those services by such third parties in a manner consistent with the requirements of this CPS.

3.2.13. Subscriber Obligations

In all cases, the Telstra Root CA shall require the Subscriber to enter into an enforceable contractual commitment for the benefit of Relying Parties obligating the Subscriber to:

- Ensure any information required to be submitted to an Issuing 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 unauthorized 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 authorized and legal purposes, consistent with this Policy;
- Request the Telstra Root CA to revoke the Certificate promptly upon any actual or suspected compromise of the Subscribers private key.

3.2.14. 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. Reliance in the case of an inability to check the status shall be governed by any contract between the parties and by applicable statute.

3.2.15. PKI Governance Council Obligations

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

3.3. Private Key Protection and Cryptographic Module Engineering Controls

The certificate holder must protect its private keys from disclosure.

3.3.1. Cryptographic Module Engineering Controls

3.3.1.1. Confidentiality/Encryption Certificates

All CA cryptographic operations will be performed in a cryptographic module validated to at least FIPS 140-2 Level 3 or otherwise verified to an equivalent level of functionality and assurance.

All RA's cryptographic operations must be performed in a cryptographic module validated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

3.3.1.2. Digital Signature Medium Assurance Certificates

All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-2 Level 3 or otherwise verified to an equivalent level of functionality and assurance. All other CA

cryptographic operations must be performed in a cryptographic module validated to at least FIPS 140-2 Level 3 or otherwise verified to an equivalent level of functionality.

The RA Administrator Digital Signature key generation and signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 1 or otherwise verified to an equivalent level of functionality and assurance

All other RA cryptographic operations must be performed cryptographic modules rated at FIPS 140-1 Level 1 or otherwise verified to an equivalent level of functionality and assurance.

3.3.1.3. Digital Signature High Assurance Certificates

All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-2 Level 3 or otherwise verified to an equivalent level of functionality and assurance.

All other CA cryptographic operations must be performed in a cryptographic module validated to at least FIPS 140-2 Level 3 or otherwise verified to an equivalent level of functionality.

The RA Administrator Digital Signature key generation and signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

All other RA cryptographic operations must be performed cryptographic modules rated at FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

Note: Brief description Of FIPS-140 in appendix

3.3.2. Cryptographic Module Standards and Controls

If approved by Telstra Corporation Limited, Cryptographic modules may be used in the Telstra Corporation Limited PKI. Note: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

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

Telstra Root CA Private Keys are under 'm of n' multi-person control.

Dual person control shall be present for all operations concerning SCA or Telstra Corporation Limited RCA Private Keys.

There is multiple person control for CA key generation operations. For Confidentiality/Encryption Certificates there must be multiple person control for private key recovery. Two staff, performing duties associated with the roles of PKI Administrator or PKI Operations, must participate or be present.

3.3.4. Private Key Escrow

Private Key escrow is supported within the Telstra Corporation Limited PKI for email and document encryption; see 6.4.3 for restraints involved in key recovery.

3.3.5. Private Key Backup

The Private Keys of the Telstra Corporation Limited RCA are stored in hardware security modules and are backed up using further encryption. Backup copies are maintained on-site with a further copy in secure off-site storage. Private Key backup is not provided for Subscribers. Except for email encryption keys see 8.2.4

Confidentiality/Encryption Certificates

- The Issuing CA must back-up private keys. The Entity may also make a back-up of the key. Backed-up keys must be stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key.

Digital Signature Medium Assurance and High Assurance Certificates

- These keys are marked as not exportable

3.3.6. Private Key Archival

Private Keys of the Telstra Corporation Limited RCA are archived in a Secure Facility. Private Key archival must be stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key.

3.3.7. Private Key Storage on a Cryptographic Module

If a Cryptographic module is used, the Private Key of the SCA or RA 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. Telstra Corporation Limited has Deployed Luna HSMs for this Secure Storage

3.3.8. Method of activating private key

The Private Keys of the Telstra Corporation Limited RCA and of SCAs are activated by Cryptographic software following the successful completion of a login process that validates an Authorised User. The Entity must be authenticated to the cryptographic module before the activation of the private key. This authentication is in the form of PED keys to the Luna HSM

3.3.9. 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.

3.3.10. Method of destroying private key

Media containing Subscriber Private Keys should be securely destroyed by PKI manager, in the following events:

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over writing. The method of over writing must be approved by the PGC.

- floppy disks - destruction by disintegration or burning; or
- hard disks - sanitisation by overwriting in accordance with ACSI 33; or
- Other media - in accordance with recommendations in ACSI 33.

Media containing a Private Key of the Telstra Corporation Limited RCA will be securely disposed of by sanitisation by overwriting (where feasible), then supervised physical destruction in accordance with ACSI33.

3.3.11. Cryptographic Module Rating

The LunaSA is rated FIPS 140-2 Level 3, EAL4

4. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The Telstra Root CA will:

- include within any certificate it issues the URL of a web site maintained by, or on behalf of, the CA;
- ensure the publication of this CPS, on a web site maintained by, or on behalf, of the Telstra Root CA,
- ensure, directly or through agreement with a repository, that operating system and repository access controls will be configured so that only authorized 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; and
- All information to be published in the Repository shall be published promptly after such information is available to the Telstra Root CA.

4.1. Repositories

The Telstra Root 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 Root CA

The Telstra Root 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 Root CA in accordance with the requirements of Section 4.9 and 4.10
- Shall make available a copy of this CPS for Subscriber and Relying Party review.
- The repository for all Public Key Certificates issued under this Telstra Corporation Limited RCA 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-pki.pki.telstra.com.au/TelstraCPS.pdf
- Note that Certificate suspension is supported under the Relationship Certificate model as operated by Telstra Corporation Limited in this Telstra Corporation Limited PKI.
- Changes in the status of Certificates issued under this Telstra Root CA CPS, including Revocation and Expiry of Certificates will be published in the Account-01 Active Directory by the Telstra Root CA.

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 Corporation Limited Account-01 Active Directory is accessible programmatically.
- The Telstra Corporation Limited 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 a Telstra Root CA may publish information submitted by them to publicly accessible directories in association with certificate status information. The publication of this information will be within the limits of section 11.3 and 11.4. Certificate and CRL publication shall be in accordance with Section 6.2.

The Telstra Root 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, the Telstra Root 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 Root 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 Corporation Limited RCA 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 Root CA and Telstra Australia RCA CA Certificate is published on Telstra Corporation Limited's website, http://telstra-pki.pki.telstra.com.au

4.2.2. Publication of Policy and Practice Information

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

Formal notification of changes to this Telstra Corporation Limited RCA CPS will not be given to any entities. Notification of changes will be provided on Telstra Corporation Limited's website, http://telstra-pki.pki.telstra.com.au/TelstraCPS.pdf this notification method uses a "pull" model. Interested parties must exercise due care and check, on a Regular basis, the Telstra Corporation Limited website to review and monitor any changes in the Telstra Root CA CPS. Interested parties are responsible for retrieving amendments when a revised and / or amended Telstra Root 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 section 11.12. Updates to Subscriber Agreements and Relying Party Agreements, as applicable, are published as necessary.

4.3.1. Frequency of publication of this CPS

New and revised approved versions of this Telstra Root CA CPS are published promptly at http://telstra-pki.pki.telstra.com.au/TelstraCPS.pdf

4.4. Access Control

The Telstra Root CA keeps access to its public repository available to Relying Parties with the purpose of validating certificates the CA's have issued and access to this CPS. The Telstra Root 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 Root CA

5. IDENTIFICATION AND AUTHENTICATION

This Section sets out the process that Applicants go through to authenticate themselves, and register for Telstra Corporation Limited PKI Keys and Certificates. In those cases where the certificate requester will not be the certificate-owner, it also describes the requirements for establishing that the certificate requester is authorized to submit the request on behalf of the eventual certificate-owner. 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. Alternately, the request can be submitted by an agent or agent process authorized by the Telstra Root 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;
- routine Re-key;
- Re-key after Revocation; and
- Revocation requests.

5.1. Naming

5.1.1. Initial Registration

Each Entity must have unique Name.

5.1.2. Types of Name

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. Each Entity may use an

alternative name via the Subject Alternate Name field, which must also be in accordance with PKIX Part 1. The DN must be in the form of a X.501 printable String IA5String, or UTF8 name and must not be blank. The Subject names in a Telstra Root CA issued certificate shall comply with the X.500 Distinguished Name (DN) form. The Telstra Root CA shall use a single naming convention as set forth below.

Each Telstra Root CA end user certificate shall contain at least the following information:

- The "Common Name" (CN), which is the end user's real name; usually displayed ascn=John Smith, the first name and last name as entered in Telstra Corporation Corporate Directory.
- An "Organization" (O) name representing the company to which the subscriber is bound. (Telstra or Telstra business partner as defined by CA administrators.)
- One or more "Organizational Unit" (OU), which is used to distinguish between different organizational groups within an organization (for example, to distinguish between human resources, accounting, and development) Usually displayed as ou=development; and
- One or more "Domain Component" (DC), the naming attributes for Domain and DNS objects. Usually displayed as dc=DomainName.

Each Telstra Root CA device or SSL certificate shall contain at least the following information:

- The "Common Name" (CN) which is the fully qualified hostname or path used in the DNS of
- The World Wide Web or Telstra server on which the certificate is installed.
- One or more "Organizational Unit Name" (OU) which is an optional field. The OU field may be used to distinguish between different organizational groups within an organization (for example, to distinguish between human resources, accounting, and development); and
- One or more "Domain Component" (DC), the naming attributes for Domain and DNS objects.

5.1.3. Need for Names to be meaningful

The contents of each certificate Subject and Issuer name fields must have an association with the authenticated name of the Entity. In the case of individuals the Relative Distinguished Name (RDN) should be a combination of first name, surname, and optionally initials. In the case of other entities the RDN will reflect the authenticated legal name of the Entity. For Telstra business partners, the DN will also include the Organization which corresponds with the particular business partner. In the case of End Entity Organizations, the DN will reflect the authenticated legal name of the End Entity. Where a Certificate refers to a role or position, the Certificate must also contain the identity of the person who holds that role or position. A certificate issued for a device or application must include within the DN the name of the person or organization responsible for that device or application.

5.1.4. Anonymity or pseudonymity, Uniqueness of names

The Subject Name listed in a Telstra Certificate shall be unambiguous and unique for all Telstra Corporation Certificates issued by the Issuing CA and conform to X.500 standards for name uniqueness. The Subject Name listed in a Telstra Business Partner Certificate shall be unambiguous and unique for each company as represented by Organization (O). Certificates issued by the Issuing CA shall conform to X.500 standards for name uniqueness.

5.1.5. Rules for interpreting various name forms

Standard Telstra naming conventions for DNS, and Telstra Corporation Limited Active Directory apply.

5.1.6. Uniqueness of names

The subject name listed in a Certificate shall be unambiguous and unique for all certificates issued by the Telstra Root CA. and conform to X.500 standards for name uniqueness. If necessary, additional numbers or letters may be appended to the real name to ensure the name's uniqueness within the domain of certificates issued by the Telstra Root CA. Wildcard name forms are allowed as long as it is for a common domain name.

The Telstra Root CA reserves the right to make all decisions regarding Entity names in all assigned certificates. A party requesting a certificate must demonstrate its right to use a particular name. Where there is a dispute about a name in a repository not under its control, the Telstra Root CA will ensure that there is a name claim dispute resolution procedure in its agreement with that repository.

The Issuing CA will investigate and correct if necessary any name collisions brought to its attention.

5.2. AUTHENTICATION

5.2.1. Recognition authentication and roles of trademarks

The use of trademarks will be reserved to registered trademark holders. All Telstra Root CA certificate subscribers represent that the information supplied by them to Telstra Corporation, which will populate the issued certificate, does not infringe upon or violate in any way the copyrights, trademarks, service marks, trade name, company name, or any other intellectual property of any third party.

The Telstra Root CA reserves the right to make all decisions regarding entity names in all assigned certificates. In the event of a dispute only the following conditions will be considered:

- Trademark name – the disputing entity must clearly demonstrate ownership of trademark. If there is a certificate containing a trademark name that was improperly registered then the Telstra Root CA will revoke the disputed certificate and re-issue a new certificate bearing a corrected name.
- Registered or legal name – the disputing entity must clearly demonstrate ownership of registered or legal name and provide justification for dispute.

An end entity is not guaranteed that its Distinguished Name or Subject Name will contain any requested trademark. The Telstra Issuing CA is not required to subsequently issue a new certificate to the rightful owner of any name if the Telstra Issuing CA has already issued to that owner a certificate containing a DN and Subject Name that are sufficient for identification within the PKI. The Telstra Issuing CA is not obligated to seek evidence of trademarks or court orders.

5.2.2. Method to prove possession of private key

PKIX Certificate Management Protocol is suitable for this requirement. The method to prove possession of a private key shall be PKCS #10, or another cryptographically equivalent request (digitally signed request with private key). Where the Private Key is generated directly on a token or in a Key generator that safely transfers the Key to a Token, the End Entity is deemed to be in possession of the Private Key at the time of generation or transfer. If the End Entity is not in possession of the Token when the Key is generated, then the Token will be delivered immediately to the End Entity via a trustworthy method.

5.2.3. Authentication of organisation identity

Confidentiality/Encryption Certificate

All organizations and entities entering into to business agreements with Telstra Corporation, that make use of the Telstra Root 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.). Identification and authentication of the prospective Subscriber must be through one of the following means:

- The certificate application must include information about that department or organization, in a form (Certificate Signing Request), as requested by the Telstra Root CA. The details must be provided in a secure manner (i.e., secure web site or equivalent method approved by the Telstra Root CA), or via a separate written document appropriately marked as confidential.
- The CA or RA must examine documentation providing evidence of the existence of the organization;
- If a Government Entity has previously established the identity of the organization using a process that satisfies the PGC, and there have been no changes in the information presented, then the CA or RA and the prospective Subscriber may utilize privately shared information. The CA or RA must also verify the identity and authority of the individual or organization acting on behalf of the prospective Subscriber and their authority to receive the keys on behalf of that organization. The CA or RA must keep a record of the type and details of identification used.

The Telstra Root 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.

Digital Signature Medium Assurance and High Assurance Certificates Are not intended for use by organizations. 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

Another person or organization authorized to act on behalf of the prospective Subscriber may make an application for an individual to be a Subscriber. Identification and authentication of the individual must be through the following means:

Confidentiality/Encryption Certificate

A Subscriber shall be an employee of the Telstra Corporation, or other entity (contractor, device, etc) that has an employment arrangement, contract, or other legally identifiable relationship with Telstra (as agreed to in the Telstra Root 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 Root 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.

Digital Signature Medium Assurance Certificate

A Subscriber shall be an employee of the Telstra Corporation, or other entity (contractor, device, etc) that has an employment arrangement, contract, or other legally identifiable relationship with Telstra (as agreed to in the Telstra Root 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 Root 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.

Digital Signature High Assurance Certificate

- The CA or RA in the presence of the individual will compare the identity of the individual with two pieces of identification (certified copies or originals). At least one of these must be government identification containing a photograph (e.g., driver's license, non driver identification, or passport). The CA or RA must keep a record of the type and details of identification used.

Electronic Notary Digital Signature

- Same requirements as for a Digital Signature High Assurance Certificate AND proof of appropriate notary commission

5.2.5. Authentication of devices or applications

An application for a device or application to be an End-Entity may be made by an individual or organization to which the device's or application's signature is attributable for the purposes of accountability and responsibility. Identification and authentication of the applicant must follow 5.1.8 as if that individual or organization was applying for the certificate on its own behalf. The CA or RA must also verify the identity of the individual or organization making the application and its authority to receive the keys for that device or application. The CA or RA must keep a record of the type and details of identification used. The CA shall establish that the applicant is in possession of the private key corresponding to the public key submitted with the application.

5.2.6. Initial Identity Validation

A Subscriber shall be an employee of the Telstra Corporation, or other entity (contractor, device, etc) that has an employment arrangement, contract, or other legally identifiable relationship with Telstra (as agreed to in the Telstra Root 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 Root 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 MANAGEMENT LIFE-CYCLE

6.1. Certificate Management Process

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

- Certificate generation;
- Certificate operational use;
- Certificate expiry, and
- Certificate archive.

6.1.1. Certificate application

The procedures and requirements with respect to an application for a certificate are set out in this CPS. An application for a certificate does not oblige the Telstra Root CA to issue a certificate.

There are three principal types of applications for certificates:

- CA certificates,

- Individual certificates (authentication and encryption certificates) - an employee or agent of Telstra Corporation that has an employment arrangement or contract with Telstra Corporation,
- Application, device and web server (SSL) certificates.

6.1.1.1. Server Certificate Applicant

A server certificate (SSL Client, SSL Server) may be a certificate used for service or device authentication purposes. An application to acquire an application server certificate will be made by an authorized person (e.g., delegated administrator, applications administrator, hosting service, etc.). The authorized person will make the application for the certificate through an enrolment page (server-authenticated SSL session). The applicant must provide details about the client or server requesting the certificate. The following information will be required:

- Requestor identity – Client ID or DNS/FQDN name.
- Organizational Identity – company and department making the request.
- Email Address (Email address for notification)
- Server Platform and Operating System
- Business Unity approver details
- Application Name
- IP Address
- A properly formatted PKCS #10 or equivalent certificate request, including the public key
- The Administrator or Vetter may contact the applicant via either physical or electronic means to ensure the legitimacy of the certificate request.

6.1.1.2. Individual (Secure Email) Certificate Applicant

Telstra employees, contractors or other end entities as defined in section 5.1.9: Subscribers of this document may be issued messaging (Secure Email) certificates from the Telstra Root CA via a manual enrolment process. For manual enrolment, the employee or contractor will be required to use an enrolment web site. Additional information will be requested such as:

- Assigned UserID
- First Name
- Last Name
- Organization
- Email Address

The information is submitted to the appropriate CA and is placed in a queue waiting to be vetted (approved). The Vetter will review the submitted information to ensure it is accurate and that the applicant is authorized to receive a certificate. If necessary, the Vetter may contact the applicant via either physical (in person) or electronic means to ensure the legitimacy of the certificate request. Once approved the applicant may download the certificate.

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 request will require access to the CA administrative request URL (Secure SSL connection), which requires a unique identifier provided by an existing CA Administrator. The request will be manually vetted and approved by existing administrators. The request must include the following information from the requestor.

- First Name and Last Name
- Organization
- Email Address

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 Root 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 a cross-certificate

The PGC will identify the necessary procedures to apply for a cross-certificate. An application for a cross-certificate does not oblige the PGC to authorize a cross-certificate. The PGC shall review any CA's request for cross-certification and approve or deny any such request according to established procedures.

A CA requesting cross-certification will include with the application:

- Its Certificate Policy;
- An external audit inspection report validating the assurance level stated in the CP;
- The public verification key generated by the CA.

6.1.2. Enrolment process and responsibilities

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

- Certification that identification information provided to Telstra Corporation during a previous registration process is accurate;
- Agreement to the protection of related keys and passwords, and if applicable, protection of tokens;
- Agreement to the acceptable use and reliance on certificates as described in this CPS and relevant corporate service documentation;
- Obligations to verify the selection of correct certificates prior to use;
- Revocation obligations and processes;
- Agreement to lifetime of certificates; and
- 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 his/her public keys and the information submitted. The Telstra Root CA shall require that each application be accompanied by:

- Proof of identity and authorization 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 authorized administrator or by the person responsible for the system or object.

6.2.2. Approval or rejection of certificate applications

Following the validation, Telstra Root 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 Root CA shall notify the subscriber why the request was rejected.

6.2.3. Time to process certificate applications

The period of time between the receipt of a valid request for a certificate and the issuance and publishing of a certificate will be a maximum of five (5) business day subsequent to the Telstra Root CA receipt of the approved request from the provisioning process.

6.2.4. 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.

6.2.5. Actions during certificate issuance

Telstra Root CA issues certificates based on requests that are correctly formatted and properly verified according to Section 5.2. The issuance of a certificate by the Telstra Root 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 Root CA is protected by a secure process.

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

A Subscriber will be notified by the Telstra Root 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.

6.2.6. Certificate Acceptance

6.2.6.1. Conduct constituting certificate acceptance

Telstra Root 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 Root CA as set forth in this CPS, and other existing agreements between Telstra Corporation and the Telstra employee, authorized vendor or agent

Telstra Root 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 Root CA.

6.2.6.2. Publication of the certificate by the CA

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

6.2.6.3. 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.

6.2.7. Key pair and certificate usage

6.2.7.1. Subscriber private key and certificate usage

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

6.2.7.2. 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.

6.2.8. Identification and authentication for revocation request

An issuing 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 his, her or 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 Root CA when faced with such a request will adopt authentication mechanisms that balance the need to prevent unauthorized 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 authorized representative of the certificate holder’s employer will always be accepted as valid Certificate Revocation and suspension

6.2.8.1. Circumstances for revocation

A certificate shall be revoked:

- When a Subscriber fails to comply with obligations set out in the Telstra Root 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 Root 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.

6.2.8.2. 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;
- A authorized executive, supervisor or administrator (Telstra Corporation PKI Governance Council) on behalf of a Subscriber or upon the Subscriber's termination;
- Personnel responsible for the operations of the Telstra Root CA.

6.2.8.3. 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

6.2.8.4. Revocation request grace period

The revocation grace period is the maximum period available, within which the Subscriber must make a revocation request upon suspicion of compromise. The grace period shall not extend beyond one Telstra business day (i.e., 8 business hours). The Telstra Root CA reserves the right to not re-issue a certificate if the grace period was not respected (i.e., negligence on behalf of the Subscriber).

6.2.9. Time within which CA must process the revocation request

6.2.9.1. 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.

6.2.9.2. CRL Issuing Frequency

The Telstra Root CA will issue a current CRL from the Issuing CA at least every 72 hours and a delta CRL every 4 hours and a current CRL from the Telstra Policy CA at least every year (or as required). In cases where a certificate is revoked, the Telstra Root CA will issue a new CRL immediately as per the requirements in Section 6.2.8.3 The Telstra Root CA will synchronize 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.

6.2.9.3. Maximum latency for CRLs

The Telstra Root 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 within minutes.

6.2.9.4. On-line revocation/status checking availability

No stipulation.

6.2.9.5. On-line revocation checking requirements

No stipulation.

6.2.9.6. Other forms of revocation advertisements available

No stipulation.

6.2.9.7. Special requirements re key compromise

No stipulation.

6.2.9.8. 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 Root CA will support certificate suspension for limited situations as determined by the Telstra Root 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.

6.2.9.9. Who can request suspension

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

6.2.9.10. Procedure for suspension request

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

6.2.9.11. Limits on suspension period

Seven Days

6.2.10. Certificate status services

6.2.10.1. Operational characteristics

The CRL will be referenced by a PKI-enabled application to verify the validity of a certificate. The Telstra Root 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. Microsoft 2003 Certificate services support HyperText Transfer Protocol (HTTP) and Lightweight Directory Access Protocol (LDAP) distribution points.

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 to the X.500 Directory.

Immediately 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.

6.2.10.2. Service availability

Telstra Root 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 Root 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.

6.2.10.3. Optional features

No Stipulation

6.2.10.4. 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.

The period of time between the receipt of a valid request for certificate revocation and the processing of a certificate revocation will be within the current business day (i.e., within 8 business hours); however immediate action is expected.

6.3. Identification and Authentication for Re-key Requests

6.3.1. Routine Re Key (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. Within six weeks prior to the scheduled expiration of the operational period of a Certificate issued following authentication under this Policy, 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.

6.3.1.1. Who may request renewal

The Telstra Root 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.

6.3.1.2. Processing certificate renewal requests

The Subscriber shall be tightly bound to their public keys and the information submitted. The Telstra Root 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.

6.3.1.3. Conduct constituting acceptance of a renewal certificate

Telstra Root 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 Root CA as set forth in this CPS, and other existing agreements between Telstra Corporation and the Telstra employee, authorized vendor or agent

Telstra Root 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 Root CA.

6.3.1.4. Publication of the renewal certificate by the CA

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

6.3.1.5. 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.

6.4. Certificate re-key

6.4.1. Circumstance for certificate re-key

Routine re-key is not supported. Prior to the expiry of a public/private key pair, an authorized individual representing the particular public/private key pair that is about to expire will be required to make a new certificate request.

Telstra Root CA, or an RA on behalf of the CA, shall authenticate all requests in the same manner as the initial application.

6.4.1.1. Re-Key after revocation – No Key Compromise

Where the information contained in a certificate has changed a CA must authenticate a re-key in the same manner as for initial registration. The CA or the RA authorized to act on behalf of that CA will verify any change in the information contained in a certificate or the RA authorized to act on behalf of that CA before that certificate is issued. The Telstra Root CA will verify any change in the information contained in a certificate before the certificate is issued.

When a Subscriber's certificate has been revoked as a result of non-compliance with Telstra Root CA CPS or Subscriber agreement, the CA/RA administrator must verify that the reasons for non-compliance have been addressed to the Telstra Root CA's satisfaction prior to certificate reissuance. The Telstra Root CA will record all requests including name of requestor, date, time, and action taken.

6.4.1.2. Re-Key after revocation – Key Compromise

Where there is a known or suspected compromise of the private key, a CA will authenticate a re-key in the same manner as for initial registration. The CA or the RA authorized to act on behalf of that CA will verify any change in the information contained in a certificate or the RA authorized to act on behalf of that CA before that certificate is issued.

6.4.1.3. Special requirements re-key compromise (CA Signing keys)

In the event of the compromise, or suspected compromise, of a CA signing key, the CA will immediately notify all CAs to whom it has issued cross-certificates and the PGC. The Telstra Policy CA1 will then revoke the issuing CA's certificate and immediately publish a new CRL. In the event of the compromise, or suspected compromise, of any other Entity's signing key, an Entity must notify the Issuing CA immediately. Telstra Root CA will ensure that it's CPS or a publicly

available document and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

6.4.1.4. Who may request certification of a new public key

No stipulation.

6.4.1.5. Processing certificate re-keying requests

No stipulation.

6.4.1.6. Notification of new certificate issuance to subscriber

No stipulation.

6.4.1.7. Conduct constituting acceptance of a re-keyed certificate

No stipulation.

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

No stipulation.

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

No stipulation.

6.4.2. Certificate modification

6.4.2.1. Circumstance for certificate modification

A certificate may be modified:

- When the basis for any information in the certificate changes.
- A change in the business relationship under which the certificate was issued occurs.

6.4.2.2. Who may request certificate modification

The modification of a certificate may only be requested by:

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

6.4.2.3. 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 Root CA shall be recorded and retained as required. The processing of a certificate modification will generally consist of the revocation of the certificate and a new certificate request performed.

6.4.2.4. 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.

6.4.2.5. Conduct constituting acceptance of modified certificate

Telstra Root 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 Root 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.

6.4.2.6. Publication of the modified certificate by the CA

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

6.4.2.7. 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.

6.4.3. Key escrow and recovery

6.4.3.1. Key escrow and recovery policy and practices

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 shall be multiple person control for key recovery operations.

There will be no key escrow of device or web server SSL private keys.

6.4.3.2. 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 Root CA. Subscribers shall satisfy the security requirements as documented in this CPS prior to certificate issuance.

The Telstra Issuing CA's 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 CA is housed in a Secure Facility operated to the level of HIGHLY PROTECTED as defined in ASIC33. The Secure Facility is staffed on a 24 x 7 basis.

- The Telstra Issuing 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 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 Issuing CA's is a locked enclosure with dual control authentication to which only PKI service operational authority personnel have physical access. The class C 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 Root 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 PGC 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 Corporation Limited 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 Root 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

Paper documents and magnetic media containing any Private Keys or commercially sensitive or Confidential Information are securely disposed of by:

In the case of magnetic media:

- physical damage to, or complete destruction of the asset; or
- The use of an approved utility to wipe or overwrite magnetic media; and in the case of printed material, cross-cut shredding.

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

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 Corporation Limited PKI contains a number of designated 'positions of trust'. These positions underpin the secure and reliable operation of the Telstra Corporation Limited 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 Root 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 Root 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 Root CA 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 the CA system 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 Governance Council 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 users keys, revocation of certificates, and renewal of certificates. The Certificate Manager Role is staffed by a Telstra PKI Governance Council authorized personnel.

7.2.1.3. Auditor

This is a role within the CA system 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 Issuing 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 Root 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 Root 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 Issuing 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 Issuing 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 Issuing 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 Corporation Limited PKI operations. In particular:

- the appropriate Security Manager always remains separate from the Telstra Corporation Limited PKI System Operators in order to provide an independent third party when reviewing and auditing Telstra Corporation Limited PKI Operations;
- logical access controls for Telstra Corporation Limited 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 Corporation Limited 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 Issuing 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 Root 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 Root 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 Issuing CA's 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 Corporation Limited PKI the following roles are to be undertaken by different personnel:

- the Telstra Corporation Limited PKI hosting facility Security Administrator will normally remain separate from the Telstra Corporation Limited 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 Issuing 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 Root CA requires that all personnel performing duties with respect to the operation of Telstra Corporation PKI have sufficient qualification and experience in PKI. 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 Root 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;

PGC 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 Policy 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 PGC may establish additional requirements conforming to state law and policy.

7.3.3. Training requirements

Telstra Issuing 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 Corporation Limited PKI concepts;
- the use and operation of the all Telstra Corporation Limited PKI software versions in use on the system;
- Telstra Corporation Limited PKI hosting facility procedures; computer security awareness and procedures, and
- The meaning and effect of this Telstra Root CA CPS.

A formal training program, founded on competency-based training principles shall be in place. The Telstra Corporation Limited PKI operation centre 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 Root 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 Root 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 Root CA, Telstra Corporation PKI Governance Council 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 PGC, 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 Root 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 Root 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 Corporation Limited PKI include (but are not limited to):

- connecting private computers, computer peripherals, or computer software to the Telstra Corporation Limited PKI network;
- Installing unauthorised software (including copyright infringed items). All software installations must be in accordance with the requirements of Telstra Corporation Limited PKI policies and the documented change management procedures;
- using Telstra Corporation Limited 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 Corporation Limited PKI hardware or software without approval of the Telstra Corporation Limited Telstra Corporation Limited PKI Security Administrator and the Telstra Australia PGC.

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, HR policies etc as Telstra employees.

Casual Telstra Corporation Limited 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 PGC.

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 Root 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 Corporation Limited PKI is largely composed of commercial-off-the-shelf products. Software documentation is therefore widely available to Telstra Corporation Limited PKI personnel. General documents relating to the operation of the Telstra Corporation Limited PKI such as this Telstra Root 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/TelstraCPS.pdf

7.4. Audit Logging Procedures

Audit log files are generated for all events relating to the security of the Telstra Root 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 RA's 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 Root 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 Root 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 Root 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 Root 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 Root 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 Root 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 Root 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 Root 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 Root 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 Root 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 Root 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 Root 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 Root 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 Root CA and subordinate SCAs in a Secure Facility.

7.6. Key Changeover

Key changeover will be affected in such a manner as to cause minimal disruption to Subscribers and End User-Subscribers.

Telstra Issuing CA's shall each obtain a new Authentication Key Pair a minimum of two years prior to the expiry of the Certificate associated with their respective current Private Authentication Key, and then commence signing new Certificates with the new Private Authentication Key.

Telstra Issuing CA's key changeover is based on CA certificate life of 5 years. If a new Telstra Issuing CA key changeover is required, the CA shall generate a new key pair and submit the certificate to the Telstra Policy CA (as per the original Key signing Ceremony) for signature. There shall be a key changeover period where the Telstra Root CA phases out the previous CA private key and public certificate. The Telstra Issuing CA private key shall not be used to sign issued certificates with a lifetime greater that the lifetime of the Telstra Issuing CA private key.

When a subscriber certificate or key pair is compromised, a new key pair shall be generated and submitted to the appropriate Issuing CA with regard to the application to replace the compromised certificate. The compromised key pairs shall be removed from the web browser, smartcard, server or device and destroyed, except if the compromised keys are used for data encryption, in which case these keys will remain on the subscriber computer, device, or smart card until such time as data previously encrypted with these keys is converted to a new encryption key pair or the user has not further need for them.

A Subscriber may only apply to renew his or her key pair within three months prior to the expiration of one of the keys, provided the previous certificate has not been revoked. A Subscriber, the CA, or the RA may initiate this key changeover process. Automated key changeover is permitted. Subscribers without valid keys must be re-authenticated by the CA or RA in the same manner as the initial registration.

When a Subscriber's certificate has been revoked as a result of non-compliance with Telstra Root CA CPS or Subscriber agreement, the Telstra Root CA must verify that the reasons for non-compliance have been addressed to the CAs satisfaction prior to certificate re-issuance.

Keys may not be renewed using an expired Digital Signature key.

The Telstra Corporation Limited PKI is committed to ensuring that Key changeover causes minimal disruption to Subscribers; and Providing Subscribers with reasonable notice of planned Key changeover.

7.7. Compromise and Disaster Recovery

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

7.7.1. Incident and compromise handling procedures

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

7.7.2. 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.

7.7.3. Entity private key compromise procedures

In the situation that the Telstra Root CA or the Telstra Policy CA or any other SCA 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 PGC and Telstra CSI shall be notified as soon as practicable;
- All subscribers shall be notified as soon as practicable; and
- Further action determined by the Telstra PGC shall be implemented.

In the event of the compromise of a CA's Digital Signature key, prior to re-certification within the Telstra Corporation Limited 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 and ARLs 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 Root 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.

7.7.4. Business continuity capabilities after a disaster

Telstra Root 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.

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

In the event of the need for revocation of a Confidentiality/Encryption certificate, the Telstra Root CA will include the Certificate serial number on an appropriate CRL. The Telstra Root 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.

7.8. Telstra Corporation Limited PKI Termination

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

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

7.8.1. CA or RA termination

In the event that Telstra Root 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 PUB 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 Corporation Limited RCA 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 root 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 Root 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

8.1.5. Key sizes

- The Telstra Root 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 Root CA

8.1.6. Public key parameters generation and quality checking

8.1.6.1. CA key generation

Telstra Root 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 PUB 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 Corporation PKI Governance Council.

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 Issuing 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.
- End User Private Keys and certificates (digital signature certificate and encryption certificate) may be used for authentication, secure email, file encryption and document/form signing.
- Digital Signature Medium Assurance and High Assurance Certificates Keys may be used for authentication, non-repudiation and message integrity. They may also be used for session key establishment.
- 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.
- Digital Signature Medium Assurance Certificates CA Digital Signature key pairs must be generated in a hardware cryptographic module.
- Key pairs for all other Entities may be generated in a software or hardware cryptographic module.
- Digital Signature High Assurance Certificates The generation of Digital Signature keys for all Entities must be generated in a 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 Root 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 Corporation Limited 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 Root CA will back up all CA private signing keys in a secure manner to support disaster recovery operations and as detailed in the Telstra Root 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 Root 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. Private Key storage on cryptographic module

The CA digital signature key is stored on a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3.

8.2.8. Method of activating private key

The Private Keys of the Telstra Corporation Limited RCA 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.

8.2.9. 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.

8.2.10. Method of destroying private key

Upon termination of use of a private key, over-writing must securely destroy all copies of the private key in computer memory and shared disk space.

Media containing Private Keys should be securely destroyed, in the following events:

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over writing. The method of over writing is approved by the PGC. Private key destruction procedures as below:

- floppy disks - destruction by disintegration or burning; or
- hard disks - sanitisation by overwriting in accordance with ACSI 33; or
- Other media - in accordance with recommendations in ACSI 33.

Media containing a Private Key of the Telstra Corporation Limited RCA will be securely disposed of by sanitisation by overwriting (where feasible), then supervised physical destruction in accordance with ACSI33.

8.2.11. Cryptographic Module Rating

CA digital signature key generation, CA digital signature key storage and certificate signing operations are performed in a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3.

8.3. Other Aspects of Key Pair Management

8.3.1. Public key archival

The Telstra Root 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 Root CA shall retain all verification public keys for 7 years.

8.3.2. Certificate Operational Periods and Key Pair Usage Periods

The Telstra Root 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 3 years (3) years;

8.4. Activation Data

8.4.1. Activation data generation and installation

All passwords used by the Telstra Root 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 Root 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 Root 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 Root CA server shall include the following functionality:

- Access control to CA services and PKI roles;
- Enforced separation of duties for PKI roles;
- Identification and authentication of PKI roles and associated identities
- Use of cryptography for session communication and database security, mutually authenticated and encrypted sessions are used for all external communications;
- Archival of CA and end entity history and audit data;
- Audit of security related events;
- Trusted path for identification of PKI roles and associated identities, use of X.509 certificates for all CA administrators; and
- 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 Root 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 Root CA. CA software, when first loaded shall provide a method for a Telstra Root 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 Root 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 Governance Council. The Telstra Root CA configuration management plan is detailed in the Telstra Root CA Operating Procedures.

8.6.3. Life cycle security ratings
No stipulation.

8.7. Network Security Controls

The Telstra Root CA server is protected by appropriate network security controls. Network security controls will permit only authorized access to the Telstra Root CA servers. Auditing will be enabled and checked on a frequent basis. Remote access to the Telstra Root 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 authorized personnel.

8.8. Time-stamping

No trusted time source is required for Telstra Root CA operations. The requirement for time-stamping of data is applicable to archives as described in section 5.5.5.

9. CERTIFICATE AND CRL PROFILES

9.1. Certificate Profile

9.1.1. Version number(s)

Telstra Root CA shall issue X.509 Version 3 certificates, 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.

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

Additionally,

Every DN must be in the form of an X.501 printableString.

9.1.2.1. CA Certificates

- The Telstra Root 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 Policy 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 Issuing 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 Root 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

9.1.2.3. Individual Certificates

- The Telstra Root CA will support the following extensions for its End User Authentication and S/MIME Digital Signature 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	URL and LDAP query
Key Usage	No	Digital Signature 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 Signature Only

- The Telstra Root 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 Root CA shall use and Subscribers shall support, for signing and verification, the following:

- RSA 2048 algorithm in accordance with PKCS#1; and/or
- SHA-1 algorithm in accordance with FIPS PUB 180-1 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 Root CA supports the use of the Policy Constraints extension.

9.1.8. Policy qualifiers syntax and semantics

Telstra Root 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 Root 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. CRLK issuance frequency

Telstra Root CA shall issue X.509 version 2 CRLs in accordance with the RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile' dated April 2002. The following represents the base CRL fields supported.

Field	Description
Version	2
Signature Algorithm	The algorithm identifier for the algorithm used to sign the CRL.
Issuer Name	Identifies the entity that signed and issued the CRL.
Effective Date	This field indicates the issue date of this CRL.
Next Update	The date by which the next CRL will be issued.

Revocation List	Revoked certificates are listed; unless there are no certificates revoked in which case the field is absent

9.2.2. 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 Root 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 PGC will authorise audits for compliance where necessary. A compliance audit determines whether a CA's performance meets the standards established in this CPS. The Policy Authority shall outline specific requirements for a compliance audit. These requirements will conform to any statutory or regulatory requirements of the Commonwealth of Australia. Before initial approval as an Approved CA, and thereafter as deemed necessary by the PGC (as applicable), shall submit to a compliance audit by an independent nationally recognized security audit firm that is approved by the Gatekeeper authority as being qualified to perform such an audit and that has significant experience in the application of PKI and cryptographic technologies.

A Compliance Audit provides an independent third party attestation that the Telstra Root CA is operating as stated in this CPS.

The purpose of such audit shall be to verify that the Telstra Root CA and its delegated parties have a system in place:

- to assure the quality of the CA services provided,
- that the CA complies with all of the requirements of this CPS, and
- That assures the CA's CPS is consistent with the requirements of this Policy and any related agreement with the PGC.
- Must have a Compliance Audit performed at their expense to demonstrate compliance with the Telstra Root CA CPS.

10.1. Frequency of entity compliance audit

A Compliance Audit will be performed 6 months from the issuance of the PKCS #7 Certificate signing process and every 12 months thereafter as required as part of the Gatekeeper Authority

The annual compliance audit will determine whether the Telstra Root CA functioning (business practices and controls) meets the requirements of this CPS.

10.2. Identity / qualifications of auditor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with requirements which the Gatekeeper Authority imposes on the issuance and management of all certificates, and which Telstra Corporation imposes on the issuance and management of their certificates. The Compliance Auditor should perform such Compliance Audits as a primary responsibility.

The Compliance Auditor will be independent of Telstra Corporation and will have proper credentials to positively identify the Compliance Auditor as belonging to a recognized audit firm.

Internal audits will be conducted by a qualified physical and logical security auditor.

10.3. Auditor's relationship to Telstra Corporation Limited RCA

External auditors will be a private firm, which is organisationally independent of the Telstra Root CA and Telstra Corporation and any subsidiaries and shall not have any current or planned financial, legal, or other relationship that could result in a conflict of interest during the period of the audit. Internal auditors will be organisationally independent of the Telstra Corporation Limited RCA's operations. The PGC shall determine whether a Compliance Auditor meets this requirement.

10.4. Topics covered by audit

The areas of the Telstra Root CA to be audited include, but are not limited to:

- compliance with Documents, Policies, Criteria and processes;
- plans, including but not limited to security, business continuity and disaster recovery plans;

- physical and logical security;
- vetting of operational personnel and personnel management;
- technology;
- data and information management;
- management of Telstra Corporation Limited PKI services; and
- Privacy.
- Telstra Root CA business practices disclosure;
- Service integrity (including key and certificate life cycle management activities);
- Telstra Root CA environmental controls.

10.5. Actions taken as a result of deficiency

When the Compliance Auditor finds a discrepancy between how the Telstra Root CA is designed, being operated or maintained, and the requirements of this CPS, the following actions may be taken depending on the severity of the discrepancy/discrepancies:

- If the discrepancy is minor, the Compliance Auditor shall note the discrepancy as part of the Compliance Audit report;
- If the discrepancy is of magnitude to deny a successful compliance audit, the Compliance Auditor shall meet with Telstra Corporation PKI Governance Council promptly. The Telstra Root CA will determine how to remedy the discrepancy and discuss with the Compliance Auditor if the remedy is sufficient to gain or retain compliance audit approval. As agreed upon by Telstra Corporation, Gatekeeper and the Compliance Auditor, an action plan with a distinct timeframe for implementing the remedy and a final report detailing the discrepancy, remedy and final outcome will be required. A final decision by the Compliance Auditor will be binding and if, in the judgment of the Compliance Auditor, the discrepancy is still severe, failure qualified audit report will be issued.

If, based on the results of the Audit report, Gatekeeper authority believes that the Telstra Root CA is not in compliance with this CPS, the Gatekeeper authority may, at its discretion,

- indicate the irregularities, but allow the CA to continue operations until the next programmed audit; or
- allow the CA to continue operations for a maximum of thirty days pending correction of any problems prior to revocation; or
- downgrade the assurance level of any cross-certificates; or
- Direct the Telstra PGC to revoke the Telstra Root CA's certificate
- Any decision regarding which of these actions to take will be based on the severity of the irregularities

When irregularities are found after an internal audit of the Telstra Root CA, the Telstra Corporation Limited PGC Chair shall promptly oversee or implement appropriate corrective action.

10.6. Communication of results

The Compliance Auditor will produce a Compliance Audit Report. The compliance audit report will be used by the Telstra Root CA to demonstrate a good standing in its practices and procedures The Compliance Audit Report will be released to the Gatekeeper Authority. All audit reports to include any corrective action taken will remain the sole property of Telstra Root CA and will be treated as confidential and protected accordingly. The results will not be made public unless required by law or a contractual agreement between Telstra Corporation and the company being given access to the report.

11. OTHER BUSINESS AND LEGAL MATTERS

11.1. Fees

11.1.1. Certificate Issuance or Renewal Fees
No fees are to be charged at this time, in future a fee structure may be introduced and this change will be reflected in the CPS and the updated document made available at

Http://telstra-pki.pki.telstra.com.au/telstraCPS.pdf

11.1.2. Certificate Access Fees
No fees are to be charged at this time, in future a fee structure may be introduced and this change will be reflected in the CPS and the updated document made available at

Http://telstra-pki.pki.telstra.com.au/telstraCPS.pdf

11.1.3. Revocation or Status Information Access Fees
No fees are to be charged at this time, in future a fee structure may be introduced and this change will be reflected in the CPS and the updated document made available at

Http://telstra-pki.pki.telstra.com.au/telstraCPS.pdf

11.1.4. Fees for Other Services
No fees are to be charged at this time, in future a fee structure may be introduced and this change will be reflected in the CPS and the updated document made available at

Http://telstra-pki.pki.telstra.com.au/telstraCPS.pdf

11.1.5. Refund Policy
No refund will be made at this time, in future a fee structure may be introduced and this change will be reflected in the CPS and the updated document made available at

Http://telstra-pki.pki.telstra.com.au/telstraCPS.pdf

11.2. Financial Responsibility
Nothing in this section affects the limitations and exclusions of liability or indemnities described in any separate agreement with Telstra, which will continue to apply in accordance with their terms.

11.2.1. Insurance Coverage
Telstra Root CA has a self-insurance license pursuant to the Safety, Rehabilitation and Compensation Act 1988 (Cth) and, due to its financial strength giving it an ability to absorb many financial risks, has elected to internally manage and self-insure any professional indemnity liabilities arising from the professional activities and operations undertaken by it in connection with this CPS.

11.2.2. Other Assets
Other assets are not addressed under this CPS.

11.2.3. Insurance or other warranty coverage for End entities
No warranty coverage is made available to Subscribers or Relying Parties under this CPS.

11.2.4. 9.2.4 Relationship
Nothing in this CPS makes either, Telstra Root CA, or the Subscriber a trustee, principal, agent, fiduciary, or representative of the other. Telstra Root CA makes no express or implied representation to the contrary.

11.3. Confidentiality of Business Information

11.3.1. Scope of Confidential Information
Subscriber information, not appearing in certificates and in public directories, held by Telstra Root CA, or an associated RA (e.g. registration and revocation information, logged events, correspondence between Subscriber and CA, etc.) is considered confidential to the Subscriber and shall not be disclosed by the Telstra Root CA except:

a) With the prior consent of the Subscriber;
b) To its officers, employees and personnel, as may be required to perform the functions of Telstra Root CA described in this CPS; or
c) As required by law or the rules of any stock exchange on which its securities are listed.

Audit information is to be considered confidential and shall not be disclosed to anyone for any purpose other than audit purposes, for the purposes described above or as permitted to be disclosed under an agreement between Telstra Corporation and the company being given access to the report.

Information pertaining to Telstra Root CA' management of a Subscriber's certificate may only be disclosed to the Subscriber or as otherwise permitted under paragraphs (a) to (c) of this section 11.3.1. Any request for the disclosure of information under paragraph (a) above shall be signed and delivered in writing to the Telstra Root CA.

The digital signature and/or authentication private Key of each Subscriber, and the Subscriber's copy of their private Key, is to be held only by the Subscriber and shall be kept confidential by them. Any disclosure of the private Key or media containing the private Key by the Subscriber is at the Subscriber's own risk.

The Subscriber shall also keep confidential the Subscriber's copy of their confidentiality Private Key. Disclosure by the Subscriber is at the Subscriber's own risk. Confidentiality Keys may be backed up by the issuing CA in which case the terms of section 6 will apply. Telstra Root CA will not disclose Confidentiality Keys without prior consent of the Subscriber or a duly authorized representative of the issuing CA unless required by law or as otherwise permitted under paragraphs (a) to (c) of this Section 11.3.1.

11.3.2. Information Not Within the Scope of Confidential Information

Certificates, CRLs, and personal or corporate information appearing in them and in public directories are not considered confidential information. Additionally, the following shall not be considered to be confidential information of a party:

- Information that is documented by the receiving party as having been independently developed by it without reference to or reliance on the confidential information of the disclosing party;
- Information that the receiving party lawfully receives from a source other than the disclosing party;
- Information that is in or enters the public domain other than because of a breach by the receiving party of this CPS;
- Information that at the time of disclosure to the receiving party was known to the receiving party as not subject to an obligation of confidentiality to the disclosing party, as evidenced by documentation in the receiving party's possession; or
- Information that the disclosing party agrees in writing is not subject to an obligation of confidentiality.

11.4. Privacy of Personal Information

11.4.1. Privacy Plan

Telstra Root CA will comply with the Privacy Act 1988 (Cth), and the Telstra Corporation Privacy Policy and Telstra Privacy Principles, as published by Telstra from time to time at the links available at http://www.telstra.com.au/privacy/privacy_telstra.html, in relation to the collection, use and disclosure of the personal information of its Subscribers, customers, employees and partners.

11.4.2. Information Treated as Private

Personal information, not appearing in certificates and in public directories, held by a CA or an RA (e.g. registration and revocation information, logged events, correspondence between Subscriber and CA, etc.) is considered private and shall not be disclosed by the CA or RA.

11.4.3. Information not treated as private
Information that is or has become publicly available (other than through an act or omission of the CA or RA), appearing in certificates and in public directories, is not considered personal information and may be disclosed subject to applicable laws.

11.4.4. Responsibility to Protect Private Information
Telstra Root CA shall keep personal information physically and/or logically protected from unauthorised viewing, modification or deletion. In addition, the CA shall ensure that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

11.4.5. Notice and consent to use private information
Personal information will only be used, collected or disclosed consistently with section 11.4.1 and as may be required under section 11.4.6.

Any request for consent to the disclosure of personal information shall be signed by the requester and delivered in writing to the Telstra Root CA

11.4.6. Disclosure pursuant to judicial or administrative process
A party may disclose personal information in compliance with any order of a court or tribunal, to the extent required by the terms of the relevant order, and to comply with any other direction of a legal or regulatory authority with which compliance is mandatory.

11.4.7. Other information disclosure circumstances
Other requirements may apply as stated in the CPS under which the Certificates are issued.

11.5. Intellectual Property Rights
The private Key shall be the sole property of the legitimate holder of the corresponding public Key identified in a Certificate.

Telstra Root CA retains all intellectual property and other proprietary rights in and to the Certificates and revocation information that is issued and Telstra Corporation retains all intellectual property rights in and to Telstra Root CA CPS. Each of Telstra Issuing CA and Telstra Corporation will respectively own, on and from creation, all intellectual property and other proprietary rights in any developments, modifications or enhancements made to those items from time to time. Subscribers and Relying Parties must ensure that such materials are, to the extent practicable, identified as the property of Telstra Root CA and Telstra Corporation (as applicable) and remain free of any lien, charge, encumbrance or other third party interest.

11.5.1. Telstra Corporation Limited Materials
Telstra Corporation Limited Materials include, but are not limited to:

- The Telstra Corporation Limited Root Certification Authority Certificate and Keys;
- This Telstra Corporation Limited Root Certification Authority Certification Practice Statement (Telstra root CA CPS);
- The Telstra Corporation Limited Subordinate Certification Authorities (Telstra Corporation Limited SCA) Certificate and Keys;
- The contents of the Account-01 Active Directory;
- any other data or database created by the Telstra Root CA, the Telstra Corporation Limited SCA, the Card Management System or Telstra Corporation Limited 's contractors and subcontractors for the purposes of the Telstra Corporation Limited PKI;
- All Certificate Policies for all PKI communities;
- All Applications and Terms and Conditions between Telstra Corporation Limited and the Subscribers in Telstra Corporation Limited PKI communities; and

- All other Documents owned by Telstra Corporation Limited and published on the Telstra Corporation Limited website for the purposes of the Telstra Corporation Limited PKI (but not including non-Telstra Corporation Limited Materials),
- Intellectual Property Rights in Telstra Corporation Limited Materials and in any modifications or enhancements made to Telstra Corporation Limited Materials remain, or are from the date of creation, the property of the Telstra Corporation Limited.
- The Telstra Root CA, Telstra Corporation Limited SCA, Telstra Corporation Limited, Subscribers and Relying Parties must ensure that Telstra Corporation Limited Materials are, to the extent practicable, identified as the property of Telstra Corporation Limited (for the Commonwealth) and that Telstra Corporation Limited Materials remain at all times free of any lien, charge or other encumbrance of a third Party.

11.6. Representations and Warranties

Telstra Root CA will issue and revoke Certificates, operate its certification and repository services, and issue CRLs, in accordance with the RSA RSS CP and this CPS. Authentication and validation procedures will be implemented pursuant to sections 5 and 6 of this CPS.

11.6.1. Telstra Corporation Limited Representations and Warranties

Telstra Root CA will conduct itself in accordance with this CPS and applicable laws, as described in section 11.14 and 11.15, when issuing and managing certificates provided to Subscribers. Telstra Root CA will require that all RAs, operating on its behalf, will comply with this CPS to the extent its terms relate to the operations and procedures of the RAs. The liability of Telstra Root CA is subject always to section 11.8.

When Telstra Root CA publishes a Certificate, it declares that it has issued a Certificate to a Subscriber and that the information stated in the Certificate was verified in accordance with sections 3 and 4 of this CPS.

CA personnel associated with PKI roles shall be individually accountable for actions they perform. "Individually accountable", means that there shall be evidence (logs) that attributes an action to the person performing the action. Records of all actions carried out by CA personnel shall identify the individual who performed the particular duty.

Telstra Root CA, under this CPS, will take reasonable commercial efforts to make Subscribers and Relying Parties aware of their respective rights and obligations with respect to the operation and management of any Keys, and/or Certificates used in connection with the Telstra Root CA. Telstra Root CA may also notify Subscribers from time to time as to, and Subscribers must comply with, procedures for dealing with suspected Key compromise, Certificate or Key renewal, and service cancellation.

11.6.2. RA representations and warranties

All RAs performing Subscriber registration tasks on behalf of Telstra Root CA must comply with all relevant provisions this CPS and any other corporate applications and services documentation outlining Telstra Corporation requirements.

The RA is responsible for the identification, authentication, and authorization of Subscribers, on behalf of Telstra Root CA, in accordance with section 5.1 and section 6.1, for certificate requests and certificate revocation requests.

RAs shall be individually accountable for actions performed on behalf of Telstra Root CA. “Individually accountable” means that there should be evidence (audit logs) that attributes an action to the person performing the action. Records of all actions carried out in performance of RA duties shall identify the individual who performed the particular duty.

When an RA submits Subscriber information to the Telstra Root CA, it shall certify to that CA that it has authenticated the identity of that Subscriber and that the Subscriber is authorised to submit a certificate request in accordance with Section 3 and Section 4.

RAs must submit certificate requests to the CA in a secure manner as described in section 5.1.

11.6.3. Other Parties Representations and Warranties

Other requirements may apply as separately agreed from time to time.

11.6.4. Subscriber representations and warranties

Subscribers registering and accepting a certificate from the Telstra Root CA must consent to a Subscribers Agreement. By utilising the delivered certificate, the Subscriber is agreeing that it has read, understood, and will abide by the terms and conditions of this CPS.

Subscribes will ensure that any Subscriber information (i.e., data required for certificate construction from either a data repository or provided by the Subscriber on the enrolment page) shall be complete and validated and contains all information required in connection with a certificate request.

11.6.5. Relying party representations and warranties

Relying Parties acknowledge they have read and accept all terms and conditions of any associated Telstra service participation agreement.

11.7. Disclaimers of Warranties

The Telstra Root CA assumes no liability except as stated in the relevant contracts pertaining to certificate issuance and management, such as a Subscriber Agreement or other relevant service agreements.

To the maximum extent permitted by applicable law, the Telstra Root CA services are provided to end entities on an 'as-is' basis, without warranties of any kind, and Telstra Root CA disclaims any and all warranties and obligations, whether express or implied, owed to third parties or end entities, including any implied warranty of merchantability, fitness for purpose, accuracy, authenticity, reliability, completeness or the currency of information provided, contained in certificates or otherwise compiled, published or disseminated and any warranty as to the non-repudiation or revocation of any Certificate or message.

If Telstra Root CA breaches any condition or warranty implied by law which cannot lawfully be excluded, then to the extent permitted by law the liability of Telstra Root CA is limited, at its option, to:

- In the case of services, the resupply of, or payment of the cost of resupplying, the service; and
- In the case of goods:
    - The replacement of the goods or the supply of equivalent goods;
    - The repair of the goods;
    - The payment of the cost of replacing the goods or of acquiring equivalent goods; or
- The payment of the cost of having the goods repaired.

11.8. Limitations of Liability

11.8.1. Certification Authority Liability

Telstra Root CA is only liable to end entities (subject always to the limitations and exclusions described in this CPS) only for loss or damage that may fairly and reasonably be considered to arise naturally in the usual course of things from: (1) the failure of the Telstra Root CA service to materially comply with the terms and conditions of this CPS, and/or (2) a material breach of any express warranty made by the corporation in this CPS, but only to the extent that such losses result

from their reasonable use of a Certificate for transactions, applications, and purposes authorized in this CPS.

Telstra Root CA excludes, and is not liable for any and all liability to any party or person for any errors, acts or omissions in connection with its provision of services or errors, acts or omissions of end entities in receiving services. Telstra Root CA is not liable for any loss:

- Of CA or RA service due to war, natural disasters or other forces or events beyond the reasonable control of Telstra Root CA;
- Incurred between the time a Certificate is revoked and the next scheduled issuance of a CRL;
- Due to fraudulent subscriber information provided by Local Registration Authorities appointed and approved by Sponsoring Organizations;
- Due to unauthorized use of certificates issued by Customer's CA, and use of certificates for any categories or types of transactions, applications or other purposes not authorised by Telstra Root CA or otherwise beyond the prescribed use defined by the certificate policy under which it was issued and this CPS;
- Due to failure of the Subscribers and relying parties to fulfil their obligations under this CPS;
- Arising from failure to protect one or more private Keys or to use a trustworthy system or otherwise prevent the compromise, loss, disclosure, modification or unauthorised use of one or more private Keys;
- Arising from the provision of any information to Telstra Root CA or to an RA by a person, organisation, or entity making application for issuance of a Certificate by the Telstra Root CA service that was false or misleading or not current, accurate, and complete at the time of submission of that information (including a failure to update an application with new material information prior to the issuance of a Certificate);
- Caused by fraudulent or negligent use of Certificates and/or CRLs issued by the Telstra Root CA service; or
- Due to disclosure of personal information contained within certificates and revocation lists. Telstra Root CA has no liability to the other party for or in respect of:
    - Any consequential, punitive, special or indirect liability, loss, damage or charge or any loss of profits, data, savings or income; or
    - Any act or omission of, or any matter arising from or consequential upon any act or omission of, any customer of the first party or any third person not under the direct control of the first party, even if Telstra Root CA has been advised of the likelihood or possibility of such liability.

11.8.2. Telstra Corporation Limited Liability

Without limitation, Telstra Corporation Limited is not liable in any way whatsoever, for any Loss whether or not reasonably foreseeable, arising in connection with the Telstra Corporation Limited PKI, including but not limited to:

- an entity described in the CPS that Certificates are issued under carrying out, or omitting to carry out, any activity described in, or contemplated by, the Documents;
- The carrying out or omitting to carry out, any activity related to the Gatekeeper accreditation process.

11.8.3. Other Parties Liability

Without limitation, RA or RAES service providers, Subscribers, Relying Parties and other participants (the Other Parties) are not liable in any way whatsoever, for any Loss whether or not reasonably foreseeable, arising in connection with the Telstra Corporation Limited PKI, including but not limited to:

- an entity described in the CPS that Certificates are issued under carrying out, or omitting to carry out, any activity described in, or contemplated by, the Documents;
- The carrying out or omitting to carry out, any activity related to the accreditation process.

11.9. Indemnities

By their applying for and being issued Certificates, or otherwise relying upon such Certificates, end entities, respectively, agree to indemnify, defend, and hold harmless the Telstra Root CA service, and its personnel, , related entities, subcontractors, suppliers, vendors, representatives and agents (each an Indemnified Person) from any errors, acts, omissions or negligence resulting in liability, losses, damages, suits, or expenses of any kind, including reasonable attorneys' fees, that an Indemnified Person may incur, that caused by the use or publication of a Certificate or the provision of any other Telstra Root CA service, that arises from:

a) their failure to provide the Telstra Root CA with current, accurate, and complete information at the time the applicant had submitted such information to the RA (including a failure to update such application with new material information prior to the CA's issuance of a certificate);
b) their errors, omissions, acts, failures to act, and negligence in receiving Telstra Root CA services from the CA, including, but not limited to, their use of certificates for any categories or types of transactions, applications or purposes not specifically authorised under this CPS; and
c) their failure to protect one or more of their private Keys, to use a trustworthy system, or to otherwise prevent the compromise, loss, disclosure, modification, or unauthorised use of one or more of their private Keys.

Each Subscriber agrees that when the Telstra Root CA issues a certificate to him/her based upon the application for such a certificate made at the request of an agent or representative of that Subscriber, the agent or representative and the Subscriber shall jointly and severally become liable, in the circumstances described above, to indemnify the Indemnified Persons pursuant to the terms of this Section 11.9. Each Subscriber also agrees that he/she has a continuing duty to immediately notify the CA of any misrepresentations, errors, or omissions made by its agent or representative in making application for and using a certificate issued by the Telstra Root CA.

11.10. Term and Termination

11.10.1. Term

This CPS continues indefinitely until the earlier of:

Notice of termination or expiry provided by Telstra Corporation at Telstra Root CA CPS' publishing point, at which time this CPS will immediately terminate;

11.10.2. Termination

This CPS will automatically terminate on publication of a newer version or replacement document by Telstra Root CA (which document will, subject to Section 11.10.3, supersede this CPS), or upon Telstra Root CA ceasing CA operations.

11.10.3. Effect of termination and survival

The conditions and effect resulting from termination of this CPS will be communicated at Telstra Root CA CPS publishing point upon termination, which communication may also outline the provisions of this CPS that may survive its termination and remain in force.

11.11. Notices and communications with participants

The Telstra Root CA may include in any separate agreement appropriate provisions governing severability, survival, merger and notices and other legal matters.

11.11.1. Publication and Notification Procedures

An electronic copy of this document, digitally signed by an authorized representative of the CA, is to be made available: At the PKI World Wide Web site,

Http://telstra-pki.pki.telstra.com.au/telstraCPS.pdf

11.12. Amendments

Telstra Corporation PKI Governance Council is the responsible authority for reviewing and approving changes to this CPS. Written and signed comments on proposed changes shall be directed to the Telstra Root CA. Decisions with respect to the proposed changes are at the sole discretion of Telstra Corporation PKI Governance Council.

11.12.1. Changes with notification

Prior to making any changes to this CPS, the PGC will notify all issuing CA's.

11.12.2. List of items

No stipulation

11.12.3. Items that can change without notification

None

11.12.4. Procedure for amendment

An electronic copy of Telstra Root CA CPS is to be made available at the Telstra web site Http://telstra-pki.pki.telstra.com.au/telstraCPS.pdf or by requesting an electronic copy by e-mail to the contact Telstra.pgc@team.telstra.com

Telstra Root CA may make changes to this CPS in its sole discretion by notification of the changes published at the above link or in such manner as prescribed by Telstra Corporation from time to time. Telstra Corporation PKI Governance Council may notify, in writing, of any proposed changes to its CPS, if in the judgment and discretion of Telstra Corporation PKI Governance Council the changes may have significant impact on the issued certificates and / or services.

The period of time that affected parties have to conform to the change will be defined in the notification.

11.12.5. Notification mechanism and period

The notification shall contain a statement of proposed changes, the final date for receipt of comments, and the proposed effective date of change. Telstra Corporation PKI Governance Council will post the notification at Telstra Root CA CPS publishing point.

Http://telstra-pki.pki.telstra.com.au/telstraCPS-notifications.pdf

11.12.5.1. Comment period

The comment period will be 30 days unless otherwise specified

11.12.5.2. Mechanism to handle comments

No Stipulation

11.12.5.3. Period for final change notice

No Stipulation

11.12.5.4. Items whose change requires a new policy

No Stipulation

11.12.6. Policy applicability

No Stipulation

11.12.7. CPS Approval Procedures

A CA's participation in the Telstra Corporation Limited PKI must be in accordance with procedures specified by the PGC. Access controls may be instituted at the discretion of the CA with respect to certificates or on-line certificate status (if the latter is provided as a service by the CA). Certificates must be published promptly upon issuance.

- The Telstra Root CA ensures, directly or with agreement with a repository, unrestricted access by Relying Parties to CRLs. The Repository will be available to Relying Parties.
- The Telstra Root CA shall not impose any access controls on this Policy, the CA's public certificate for its signing key, and past and current versions of the CA's CPS.
- The Telstra Root CA may impose access controls on Certificates, certificate status information, or CRLs at its discretion, subject to agreement between the CA and Subscriber, in accordance with provisions published in its CPS or otherwise.

11.12.8. Disaster Recovery Plan

The Telstra Root CA has in place an appropriate disaster recovery and business resumption plan. The plan will set up and render operational a facility located in a geographic diverse area that is capable of providing CA Services in accordance with this Policy with-in seventy two (72) hours of an unanticipated emergency. The plan includes a complete and periodic test of readiness for such facility. This plan is confidential and not available for general viewing.

11.12.9. Circumstances under which OID must be changed

If a policy change is determined by the Gatekeeper Authority to warrant the issuance of a new policy, the Telstra PGC will assign a new Object Identifier (OID) for the new policy and notify the Telstra Root CA.

11.13. Dispute Resolution Procedures

Any dispute related to Key and Certificate management between the Telstra Root CA and any other organization or individual outside the CA should be resolved using an appropriate dispute settlement mechanism. A dispute should be resolved by negotiations if possible. The Telstra Root CA will provide appropriate dispute resolution procedures in any agreement it enters into.

Except where a party seeks urgent injunctive or similar interim relief, the procedures contained in this Section 11.13 must be followed in relation to a dispute. If there is no dispute resolution procedure in the relevant agreement, then this section in the CPS will take precedence.

11.13.1. Negotiation

a) In the event of any dispute relating to the subject matter of this CPS, the party claiming the dispute has arisen (Initiating Party) must provide a written notice (Dispute Notice) to the other party (Recipient Party) setting out brief details of the dispute.
b) If a Dispute Notice is given, the parties must make their nominated dispute officers available for the purpose of meeting in an effort to resolve the dispute. At least one meeting of the dispute officers must take place within 10 business days of service of the Dispute Notice.
c) In the event the Recipient Party does not make its dispute officer available for a meeting within the time period set out in Section 9.13.1(b), the Initiating Party is entitled to proceed immediately with resolving the dispute pursuant the balance of this Section 9.13.

11.13.2. Dispute resolution

a) In the event that negotiation fails to resolve the dispute within thirty (30) days from the date of the relevant Dispute Notice or in the circumstances described in Section 11.13.1(c), the dispute will be submitted to mediation administered by the Australian Commercial Disputes Centre (ACDC). The mediator will have no power to bind the parties. The mediation will be confidential and without prejudice.

b) Selection of Mediator - Both parties will have three days to agree upon a mutually acceptable mediator. If no mediator has been selected both parties agree to request the Australian Commercial Disputes Centre (ACDC) to appoint a mediator.
c) The mediation is to be conducted in accordance with the latest version of the ACDC Mediation Guidelines to the extent that such guidelines are non inconsistent with any other provisions of this CPS unless the mediation is administered by an organisation other than the ACDC, in which case the mediation is to be conducted in accordance with the current guidelines of that organisation (to the extent not inconsistent with any other provision of this CPS or the Certificates issued under it).
d) In the event that the dispute has not been settled within twenty-eight (28) business days or such other period as agreed to in writing by the parties to the dispute after the appointment of the mediator, then (if the parties to the dispute agree) the dispute may be submitted to arbitration administrated by the ACDC in accordance with its current arbitration guidelines. If the parties do not agree to arbitration, then either may proceed under Section 11.13.3

11.13.3. Litigation

If the dispute is not resolved pursuant to the processes described above then either party may commence Litigation concerning the subject matter of the dispute. In the event that either party decides to litigate, litigation shall be brought in the courts of Victoria, Australia.

11.14. Governing Law

The Telstra Root CA CPS and all corresponding agreements shall be governed by the laws of Victoria, Australia.

11.15. Compliance with Applicable Law

Other requirements may apply as separately agreed from time to time.

11.16. Miscellaneous Provisions

11.16.1. Entire agreement

The Telstra Root CA will define in any applicable agreement the appropriate provisions governing severability, enforcement and waiver of rights, survival, merger and notice.

11.16.2. Assignment

Subscribers and Relying Parties may not assign any of its rights or obligations hereunder, without the written consent of Telstra Corporation PKI Policy Management Authority.

11.16.3. Force Majeure

Telstra Root CA shall not be held responsible for any delay or failure in performance of its obligations hereunder to the extent such delay or failure is caused by fire, flood, strike, civil, governmental or military authority, acts of terrorism or war, act of God, or other causes beyond its reasonable control.

11.16.4. Other provisions

Other requirements may apply as separately agreed from time to time.

12. APPENDIX A PKI WEBSITE

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

- Telstra Corporation Limited RCA CPS
- Subscriber Application and Terms and Conditions document
- The Telstra Corporation Limited PKI privacy policy

http://telstra-pki.pki.telstra.com.au

12.1. References

Document Number	Title

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

TERM: access control
DEFINITION: The granting or denial of use or entry.

TERM: 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.

TERM: 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.

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

TERM: 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."

TERM: 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.

TERM: 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".

TERM: 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.

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

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

TERM: authorization
DEFINITION: The granting of permissions of use.

B

TERM: 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

TERM: 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.

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

TERM: 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.

TERM: Certification Chain

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

TERM: 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.

TERM: 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.

TERM: 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.

TERM: 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.

TERM: 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.

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

TERM: 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

TERM: 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.

TERM: 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.

TERM: 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

TERM: 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

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

TERM: 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
TERM: 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.

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

TERM: 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.

TERM: 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.

TERM: 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
TERM: 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.

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

M

TERM: MD5

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

N

TERM: non-repudiation

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

O

TERM: Object Identifier (OID)

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

P

TERM: Personal information

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

TERM: 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.

TERM: 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.

TERM: 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.

TERM: 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.

TERM: 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.

TERM: PKI personnel

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

TERM: 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.

TERM: 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.

TERM: 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.

TERM: Public Key Infrastructure

DEFINITION: A set of policies, procedures, technology, audit and control mechanisms used for the purpose of managing certificates and keys.

TERM: Public

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

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

Q

R

TERM: 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.

TERM: 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 ROOT CA does not support rekey.

TERM: 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

TERM: Relying Party
DEFINITION: A person or entity that uses a certificate signed by the CA to authenticate a digital signature or encrypt communications to a certificate subject. The relying party relies on the certificate as a result of the certificate being sign by a CA, which is trusted. A relying party normally is but does not have to be a Subscriber of the PKI.

TERM: 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.

TERM: 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).

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

S

TERM: 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.

TERM: 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.

TERM: 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.

TERM: 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.

TERM: 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

TERM: 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)..

TERM: 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).

TERM: 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.

TERM: 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
TERM: 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

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

TERM: 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
TERM: 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.

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

TERM: vulnerability
DEFINITION: weaknesses in a safeguard or the absence of a safeguard.

W
TERM: 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

TERM: X.500

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

TERM: 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.

TERM: X.509

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

TERM: 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 C 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. ATTACHMENTS

Document Number	Title

17. DOCUMENT CONTROL SHEET

Contact for Enquiries and Proposed Changes

If you have any questions regarding this document contact:

Name: Paul Lexa

Designation: PKI Technical Specialist

Phone: 03 86472841

Fax:

If you have a suggestion for improving this document, complete and forward a copy of Suggestions for Improvements to Documentation (form 000 001-F01).

Record of Issues

Issue No	Issue Date	Nature of Amendment
1	20/09/2010	Initial Draft