TELSTRA RSS CA
Certification Practice Statement (CPS)

Last Revision Date: June 12, 2012

Version: 1.3

Published By: Telstra Corporation Ltd

REVISION HISTORY

Version	Date	Author's initials	Description of changes
0.1	3/15/2009	KR (RSA)	Initial release (DRAFT)
0.2	3/30/2009	KR (RSA)	Updates based on Telstra feedback
0.3	21/05/2009	GD (Telstra)	Updates based on discussion within Telstra PKI Project Team. Pending review from RSA.
0.4	23/05/2009	SA (Telstra)	Internal review
0.5	23/06/2009	GD (Telstra)	Updates based on RSA's feedback
0.6	27/06/2009	SA (Telstra)	Internal Review
0.7	16/07/2009	GD, SA (Telstra)	Internal Review
0.71	16/07/2009	SA (Telstra)	Revisited and cleaned up comments
0.72	30/09/2009	EL (Telstra)	Modified chapter 9 to align with Telstra legal
0.80	27/09/2009	SA (Telstra)	Internal Review
0.81	12/11/2009	CP (Telstra)	Minor formatting and spelling updates
1.0	16/12/2009	CP (Telstra)	Changes to Section 7, general formatting upgrades and promoted to release 1.0
1.1	24/7/2010	PL	Changed PGC email;
1.2	10/06/2011	AO (Telstra)	Changes made were based on E&Y recommendations during RSA RSS audit
1.3	12/06/2012	PJ (Telstra)	Changes made based on E&Y recommendations during the 2012 Audit

TABLE OF CONTENTS

CPS SPECIFICATION

1 INTRODUCTION

1.1 Overview

This Certification Practice Statement (CPS) defines the practices and procedures for the Telstra Corporation's Policy CA (Telstra RSS Policy CA) and Telstra Corporation's RSS Issuing CAs (Telstra RSS Issuing CAs), collectively named "**TELSTRA RSS CA"**, for use in creating keys for signing, and issuing end-entity (end users, device, web server and application) certificates. This CPS is in conformance with the RSA ROOT SIGNING SERVICE (RSA RSS) Certificate Policy (CP). The TELSTRA RSS CA is operated in Melbourne, Australia.

The RSA ROOT SIGNING SERVICE CP (RSA RSS CP) describes the legal, business and technical requirements for the TELSTRA RSS CA. This CPS sets forth the business, legal and technical practices and procedures for approving, managing, revoking and renewing digital certificates within the TELSTRA RSS CA environment; the CPS provides the context under which certificates are requested, created, issued, renewed, and/or used by Subscribers of TELSTRA RSS CA.

The TELSTRA RSS CA CPS generally conforms to the IETF PKIX Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework (also known as RFC 3647). This document is divided into nine sections:

- Section 1 – provides an overview of the policy and set of provisions, as well as the types of entities and the appropriate applications for certificates.
- Section 2 – 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 3 – covers the identification and authentication requirements for certificate related activity.
- Section 4 – deals with certificate life-cycle management and operational requirements including application for a certificate, revocation, suspension, audit, archival and compromise.
- Section 5 – covers facility, management and operational controls (physical and procedural security requirements).
- Section 6 – provides the technical controls with regard to cryptographic key requirements.
- Section 7 – 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 8 – 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 9 – covers general business and legal matters: the business issues of fees, liabilities, obligations, legal requirements, governing laws, processes, confidentiality, etc.

This CPS does not provide details on the operations of the TELSTRA RSS CA; rather it provides the overview of the practices. Details of the operations are found in supporting documents, such as Telstra Corporation PKI Operating Procedures.

1.2 Document name and identification

The OID for the RSA ROOT SIGNING SERVICE Certificate Policy (RSA RSS CP) is **1.2.840.113549.5.6.1**

This CPS complies with the RSA RSS CP. This CPS is titled The TELSTRA RSS CA Certification Practice Statement (CPS) or "**TELSTRA RSS CA CPS**".

1.3 PKI participants

The TELSTRA RSS CA is authorized by Telstra Corporation to create, sign, issue and manage digital certificates. Each CA is bound to act according to the terms of the RSA RSS CP and this CPS.

This CPS is applicable to the Telstra RSS Policy CA and the Telstra RSS Issuing CAs (direct subordinate CAs to the Telstra RSS Policy CA). The communities governed by this CPS are all components that reside within the TELSTRA RSS CA environment.

The Telstra RSS Policy CA will not issue end entity certificates; this CA will only issue CA certificates. Issuing CAs will issue certificates to end entities (end users, devices and servers) that have a valid business relationship with Telstra and are bound to comply with provisions of the relationship and applicable corporate policies. Authorized end entities are further defined in the Telstra-RSA Root Signing Agreement.

This CPS is applicable to all certificates issued by the TELSTRA RSS CA. The practices described in this CPS apply to the issuance, use of the certificates and the revocation of certificates of Subscribers and Relying Parties of the TELSTRA RSS CA.

1.3.1 Certificate Authorities (CAs)

The Telstra RSS Policy CA, operating under the RSA RSS CP, will certify the public keys of the Telstra RSS Issuing CAs creating a trust relationship between the Telstra RSS Policy CA and all Telstra RSS Issuing CAs.

The Telstra RSS Issuing CAs, also operating under the RSA RSS CP, may sign signature, authentication and/or confidentiality certificates that bind subscribers (end users, applications, web servers) to their private keys. The CA is responsible for:

- The creation and signing of certificates binding subscribers and PKI personnel with their authentication, signature verification and encryption public keys.
- Promulgating certificate status through publishing certificates and CRL status to publicly available repositories; and
- Adherence to this CPS and the RSA RSS CP.

The following certificate types will be recognized for use within the TELSTRA RSS CA established by this CPS. The certificate types listed below - Personal, Business and Server - vary depending on the identity of the Certificate Holder (Individual, Affiliated Individual and Electronic Device, respectively). All certificates issued under this CPS will contain the policy OID of the RSA RSS CP in the Certificate Policies extension of the Certificate:

- Personal– issued to Individuals (authentication, digital signature and encryption)
- Server Certificate– issued to SSL-enabled Electronic Devices or CA devices
-
- Other Types – as allowed by the RSA RSS CP and this CPS and upon approval of Telstra Corporation PKI Governance Council.

1.3.2 Registration Authorities (RAs)

A Registration Authority (RA) is an entity approved by a CA to assist in the verification of certificate request content (applicant information) on behalf of a CA. The primary responsibility of the RA is to verify that the party submitting the certificate request is who it claims to be and is authorized to submit the request on behalf of the certificate request origin, has a valid business relationship with Telstra, and that the certificate request has been transferred from the origin to the RA in a secure manner. An RA operating under this CPS may also be responsible for other duties delegated to it by the TELSTRA RSS CA. The RA may be tasked to verify certificate revocation requests in a similar manner; that is, verifying the party submitting the revocation request is who it claims to be and is authorized to submit the revocation request on behalf of the origin. The duties performed by an RA may be performed in a manual process or performed in an automated process so long as the integrity of the verification process is not compromised.

The TELSTRA RSS CA may assign registration functions to an organization that agrees to fulfill the functions of a Registration Authority (RA) in accordance with the terms of RSA RSS CP and this CPS. An RA operating under the RSA RSS CP and this CPS is only responsible for those duties assigned to it by the TELSTRA RSS CA pursuant to an agreement as specified in RSA RSS CP and this CPS. Either the CA or RAs operating within the TELSTRA RSS CA service may perform identification and authentication requirements.

1.3.3 Subscribers

For the purposes of this CPS a Subscriber is an entity that has been issued an end entity (end user, application or web server) certificate. In cases where the end-entity is a server or an application, an authorized individual must be responsible for the certificate and accountable for its use.

Eligibility for a certificate is at the sole discretion of the TELSTRA RSS CA.

Participants in TELSTRA RSS CA can include but are not limited to all employees or contractors of Telstra Corporation, its wholly owned subsidiaries, business divisions and authorized business partners as allowed through agreement with the RSA Root Signing Service (RSA RSS).

1.3.4 Relying parties

A Relying Party is an entity that relies on a certificate or information about the certificate that is issued by the TELSTRA RSS CA. All Relying Parties entrusted with a certificate issued by The TELSTRA RSS CA must abide by the provisions of this CPS.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

This CPS is applicable to all certificates issued and distributed by the TELSTRA RSS CA. The practices described in this CPS apply to the issuance, utilization and revocation of certificates of the TELSTRA RSS CA.

1.4.1 Appropriate certificate uses

Certificates issued under this CPS by the TELSTRA RSS CA are suitable for:

- Protecting the integrity and authenticity of business transactions as well as providing a basis for non-repudiation.
- Protecting the confidentiality of information to facilitate the confidential transfer of or restrict access to that information.

Section 7.1.2 further defines certificate usage profiles.

1.4.2 Prohibited certificate uses

Certificates issued under this CPS by the TELSTRA RSS CA are prohibited under any other use not specified in Section 1.4.1.

Certificates issued by the TELSTRA RSS CA must not be used fraudulently or in any otherwise illegal manner. A revoked or expired certificate may not be used for any purpose. No action taken by an authorized Relying Party will be considered valid unless the digital signature was created during the operational period of a valid TELSTRA RSS CA ISSUING CA issued certificate.

1.5 Policy administration

Telstra Corporation PKI Governance Council (PGC) is the overall administrative authority of this CPS.

1.5.1 Organization administering the document

The Telstra Corporation PKI Governance Council is the responsible authority for reviewing and administering changes to TELSTRA RSS CA CPS. Written and signed comments on proposed changes shall be directed to the TELSTRA RSS CA contact as described in Section 1.5.2.

1.5.2 Contact person

The following is the primary contact for the TELSTRA RSS CA:

Telstra Corporation Limited
Information Security Operations Manager
242 Exhibition St
Melbourne Victoria 3000 Australia
Email: telstra.pgc@team.telstra.com

1.5.3 Person determining CPS suitability for the policy

RSA ROOT SIGNING SERVICE is the administrative entity for determining CPS suitability to RSA RSS Certificate Policy.

1.5.4 CPS approval procedures

Telstra Corporation PKI Governance Council (PGC) will submit any proposed changes to TELSTRA RSS CA CPS to the RSA ROOT SIGNING SERVICE for review to determine if these modifications, additions or deletions are acceptable and do not jeopardize operations or the security of the RSA ROOT SIGNING SERVICE.

1.6 Definitions and acronyms

A list of definitions and acronyms can be found at the end of this document.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The TELSTRA RSS CA will have at least one certificate repository and one CRL repository, or one repository that holds 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 RSS CA.

The TELSTRA RSS 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 RSS CA in accordance with the requirements of Section 4.9 and 4.10; and
- Shall make available a copy of this CPS for Subscriber and Relying Party review.

2.2 Publication of certification information

Subscribers shall be notified that a 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 9.3 and 9.4. Certificate and CRL publication shall be in accordance with Section 4.

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

2.3 Time or 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 4 of this CPS.

Updates to this CPS are published in accordance with section 9.12. Updates to Subscriber Agreements and Relying Party Agreements, as applicable, are published as necessary.

2.4 Access controls on repositories

The TELSTRA RSS CA keeps access to its public repository available to Relying Parties with the purpose of validating certificates the CA has issued. The TELSTRA RSS 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 RSS CA with respect to certificate status. The TELSTRA RSS CA will:

- Provide, directly or with agreement with a repository provider, access to certificate repositories. Certificates will be delivered promptly upon issuance.
- Provide directly or with agreement with a repository provider access to CRLs. CRL publication will be in accordance with Section 4. Alternatively or in addition, on-line certificate status information will be provided in accordance with Section 4.
- Include within any certificate that it issues the URL of the website maintained by, or on behalf of, the TELSTRA RSS CA.

- Provide the publication of this CPS on a web site maintained by TELSTRA RSS CA, or another entity on behalf of the TELSTRA RSS CA; the location of which will be indicated in compliance with Section 9.12;
- Provide a read-only copy of this CPS to the publication point to ensure unauthorized modification are not permitted; and
- Provide full text version of the CPS when necessary for the purposes of audit, accreditation or as required by law. The location of publication of TELSTRA RSS CA CPS and updates is described in Section 9.12.

3 IDENTIFICATION AND AUTHENTICATION

This section describes the requirements for authentication of the certificate requester. 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 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.

3.1 Naming

3.1.1 Types of names

Each entity will 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 SubjectAlternateName field, which also will be in accordance with PKIX Part 1. The DN will be in the form of a X.501 printableString, IA5String, or UTF8 name and will not be blank.

The Subject names in a TELSTRA RSS CA issued certificate shall comply with the X.500 Distinguished Name (DN) form. The TELSTRA RSS CA shall use a single naming convention as set forth below.

Each TELSTRA RSS 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 as cn=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 the RSA RSS 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 RSS 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.

3.1.2 Need for names to be meaningful

The contents of each certificate Subject and Issuer name field will have an association with the authenticated name of the entity. The relative distinguished name (RDN) should reflect the authenticated legal name of the entity.

In the case of Individuals, the authenticated common name should be a combination of first name, surname, and optionally initials. 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 web server must include the authenticated name of the device or web server, and/or name of the responsible Individual or Organization or both

3.1.3 Anonymity or pseudonymity of subscribers

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.

3.1.4 Rules for interpreting various name forms

No stipulation; at the discretion of the TELSTRA RSS CA.

3.1.5 Uniqueness of names

The Issuing CA may defer to a naming authority for guidance on name interpretation and subordination. 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 RSS ISSUING CA. No wildcard name forms are allowed. The TELSTRA RSS ISSUING CA reserves the right to make all decisions regarding End Entity names in Certificates. If necessary, a party requesting a certificate may be required to demonstrate its right to use a particular name. The Issuing CA will investigate and correct if necessary any name collisions brought to its attention.

3.1.6 Recognition, authentication, and role of trademarks

All TELSTRA RSS 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 RSS 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 RSS 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 RSS 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 RSS ISSUING CA is not obligated to seek evidence of trademarks or court orders.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

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.

3.2.2 Authentication of organization identity

All organizations entering into to business agreements with Telstra Corporation, that make use of the TELSTRA RSS 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.). The certificate application must include information about that department or organization, in a form (Certificate Signing Request), as requested by the TELSTRA RSS CA. The details must be provided in a secure manner (i.e., secure web site or equivalent method approved by the TELSTRA RSS CA), or via a separate written document appropriately marked as confidential.

The TELSTRA RSS 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.

3.2.3 Authentication of individual identity

An application to acquire a certificate, to become a Subscriber, may only be requested by an authorized individual affiliated with Telstra Corporation or a Telstra Business Partner as defined by the RSA RSS Agreement. 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 RSA RSS CP), 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 Owner).

3.2.3.1 Server Certificate Applicant

A server certificate (SSL Client, SSL Server, CA device) 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.).**Manual Enrollment**
An application to acquire an application server certificate will be made by an authorized person (e.g., delegated administrator, applications administrator, etc.). The authorized person will make the application for the certificate through an enrollment page (server-authenticated SSL session) or change management process.

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)

The Administrator or Vettor may contact the applicant via either physical or electronic means to ensure the legitimacy of the certificate request.

The accuracy and completeness of the information included in the subscriber's certificate request is verified by comparing the certificate request information and certificate signing request against internal employee database and public white and yellow pages

3.2.3.2 Individual (Secure Email) Certificate Applicant

Telstra employees, contractors or other end entities as defined in section 1.3.3: Subscribers of this document may be issued messaging (Secure Email) certificates from the TELSTRA RSS CA via a manual enrollment process.

Manual Enrollment
For manual enrollment, the employee or contractor will be required to use an enrollment 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 Vettor will review the submitted information to ensure it is accurate and that the applicant is authorized to receive a certificate. If necessary, the Vettor 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.

The accuracy and completeness of the information included in the subscriber's certificate request is verified by comparing the certificate request information and certificate signing request against internal employee database and public white and yellow pages

3.2.4 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 enrollment will be not be verified for accuracy.

Telstra Corporation certificate authority reserves the right not to publish information not required for the responsible and secure operation of the TELSTRA RSS CA or issuance of the certificate. The Naming convention and conformity to the rules set forth in section 3.1 of this document as well as the identity and authentication information provided by subscribers will be considered in enrollment of digital certificates.

3.2.5 Validation of authority

The TELSTRA RSS CA shall verify the identity of the individual making the application, the validity of that individual, department and/or organization to make a certificate application, and their authority to receive the certificate(s) for that organization.

The CA verifies the authority of the subscriber to request a certificate by comparing the identity information specified in the certificate request with the information in the Certificate Signing Request (CSR), and validating this information against internal and external databases.

3.2.6 Criteria for interoperation

Cross Certification between external CAs and TELSTRA RSS CA CAs will **not** be supported.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

As long as an End Entity's certificate has not been revoked, the End Entity may, within three months prior to the end of the certificate's validity period, request issuance of a new certificate with a new Key Pair.

The TELSTRA RSS CA shall authenticate all requests for re-key, and the subsequent response shall be authenticated by the entity. The request for re-key shall be authenticated in the same manner as the initial registration.

3.3.2 Identification and authentication for re-key after revocation

Where the information contained in a certificate has changed or there is a known or suspected compromise of the private key, the CA will authenticate a re-key in the same manner as for initial registration. The TELSTRA RSS 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 RSS CA CPS or Subscriber agreement, the CA/RA administrator must verify that the reasons for non-compliance have been addressed to the TELSTRA RSS CA's satisfaction prior to certificate re-issuance.

The TELSTRA RSS CA will record all requests including name of requestor, date, time, and action taken.

3.4 Identification and authentication for revocation request

An issuing TELSTRA RSS 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 (persons permitted to submit revocation requests are detailed in section 4.9). The TELSTRA RSS CA when faced with such a request must 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.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 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 RSS 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.

4.1.1 Application for Individual certificates

Individuals, as described above, applying for certificates will follow the requirements of section 3.2.3. The Subscriber shall be tightly bound to their public keys and the information submitted.

4.1.2 Application for web or application server SSL certificate

An entity/person authorized to act on behalf of a department, organization or group within Telstra Corporation may make a request for an application server or device certificate. Administrative contact information will be identified including name, title, address, phone, and e-mail. The certificate application will follow the requirements for Sections 3.2.2 to 3.2.3 as well as fulfill the requirements of any applicable agreement.

4.1.3 Who can submit a certificate application

The TELSTRA RSS CA shall require that every Subscriber be an employee, authorized vendor (as defined in the RSS Agreement) 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 Subscriber information (i.e., data required for certificate construction from either a data repository or provided by the Subscriber on the enrollment page) shall be complete and validated with full disclosure of all required information in connection with a certificate request.

4.1.4 Enrollment process and responsibilities

Subscribers registering and accepting a certificate from the TELSTRA RSS 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 RSA RSS CP, 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.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The Subscriber shall be tightly bound to his/her public keys and the information submitted. The TELSTRA RSS CA shall require that each application be accompanied by:

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

In case the requester is a natural person requesting his or her own certificate, the procedures detailed in section 3 apply. 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.

4.2.2 Approval or rejection of certificate applications

Following the validation, TELSTRA RSS 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 RSS CA shall notify the subscriber why the request was rejected.

4.2.3 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 RSS CA receipt of the approved request from the provisioning process.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

TELSTRA RSS CA issues certificates based on requests that are correctly formatted and properly verified according to Section 3.1 and 4.2. The issuance of a certificate by the TELSTRA RSS 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 RSS CA is protected by a secure process.

4.3.2 Notification to subscriber by the CA of issuance of certificate

A Subscriber will be notified by the TELSTRA RSS 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 enrollment process.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

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

TELSTRA RSS CA 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 RSS CA.

4.4.2 Publication of the certificate by the CA

TELSTRA RSS CA is responsible for repository and publication functions. TELSTRA RSS CA shall publish certificates in a repository based on the certificate publishing practices of TELSTRA RSS CA, as well as revocation information concerning such certificates, as defined in section 4.9 and 4.10.

4.4.3 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.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

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

4.5.2 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.

Prior to using a Subscriber's certificate, a Relying Party shall verify the digital signature on the certificate.

4.6 Certificate renewal

4.6.1 Circumstance for 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. Certificate renewal will only be permitted within 3 months prior to certificate expiration. On a case by case basis, certificate renewal may be permitted when information in a certificate has changed.

4.6.2 Who may request renewal

The TELSTRA RSS 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.

4.6.3 Processing certificate renewal requests

The Subscriber shall be tightly bound to their public keys and the information submitted. The TELSTRA RSS 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.

4.6.4 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 renewal process.

4.6.5 Conduct constituting acceptance of a renewal certificate

TELSTRA RSS CA does not require notification from an end user acknowledging acceptance of a certificate renewal. The acceptance of the certificate by the subscriber is manifested by the utilization of the renewed certificate.

TELSTRA RSS CA will require that an entity acknowledge acceptance of a device or web server SSL certificate renewal. 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 RSS CA.

4.6.6 Publication of the renewal certificate by the CA

TELSTRA RSS CA is responsible for repository and publication functions. TELSTRA RSS CA shall publish renewed certificates, as per the initial enrollment, in a repository based on the certificate publishing practices of TELSTRA RSS CA, as well as revocation information concerning such certificates, as defined in Section 4.9 and 4.10.

4.6.7 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 renewed.

4.7 Certificate re-key

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

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

A certificate may be modified:

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

4.8.2 Who may request certificate modification

The modification of a certificate may only be requested by:

3. The individual, department or organization which made the application for the certificate;
4. An authorized supervisor or administrator (Delegated Administrator) on behalf of a Subscriber; or
5. Personnel of the TELSTRA RSS CA.

4.8.3 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 RSS 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.

4.8.4 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.

4.8.5 Conduct constituting acceptance of modified certificate

TELSTRA RSS 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 RSS 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 RSS CA.

4.8.6 Publication of the modified certificate by the CA

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

4.8.7 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.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate shall be revoked:

6. When a Subscriber fails to comply with obligations set out in the RSA RSS CP, this CPS, Subscriber agreement or applicable law.
7. When the basis for any information in the certificate changes.
8. A change in the business relationship under which the certificate was issued occurs.
9. 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.
10. 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.
11. When the TELSTRA RSS 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.

4.9.2 Who can request revocation

The revocation of a certificate may only be requested by:

12. The individual, department or organization which made the application for the certificate;
13. A authorized executive, supervisor or administrator (Telstra Corporation PKI Governance Council) on behalf of a Subscriber or upon the Subscriber's termination ; or
14. Personnel responsible for the operations of the TELSTRA RSS CA.

4.9.3 Procedure for revocation request

All requests for revocation shall be submitted via an on-line process or in writing to pki.operations@team.telstra.com. 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 subscriber shall be notified of such revocation. The revocation notification will be in the form of an email to the Subscriber informing of the successful completion of the revocation process

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 4.10.

4.9.4 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 RSS 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).

4.9.5 Time within which CA must process the revocation request

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.

4.9.6 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 (4.9) and section 4.10. 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.

4.9.7 CRL issuance frequency

The TELSTRA RSS CA will issue a current CRL from the Issuing CA at least every 24 hours and a current CRL from the Telstra RSA RSS Policy CA at least every year (or as required). In cases where a certificate is revoked, the TELSTRA RSS CA will issue a new CRL immediately as per the requirements in Section 4.9.5. The TELSTRA RSS CA will synchronize the CRL issuance and publishing to an external LDAP directory or web server publishing to ensure the most recent CRL is available to Relying Parties.

4.9.8 Maximum latency for CRLs

The TELSTRA RSS 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.

4.9.9 On-line revocation/status checking availability

No stipulation.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 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 RSS CA will support certificate suspension for limited situations as determined by the Telstra RSS 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.

4.9.14 Who can request suspension

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

4.9.15 Procedure for suspension request

The procedures for requesting a suspension are the same as for requesting revocation in Section 4.9.3.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

4.10.1 Operational characteristics

The CRL will be referenced by a PKI-enabled application to verify the validity of a certificate. The TELSTRA RSS CA certificates include the CRL name and distribution points as part of the certificate extension information. When a certificate is revoked or expires, 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 is at the URL defined in 4.9.6. The CRL access URL will also be provided in the detailed body of the certificate.

4.10.2 Service availability

TELSTRA RSS 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 RSS 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.

4.10.3 Optional features

No Stipulation

4.11 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.

4.12 Key escrow and recovery

4.12.1 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.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

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

The TELSTRA RSS CA is 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.

5.1.1 Site location and construction

15. The TELSTRA RSS CA is to reside in a physically secure environment.
16. To support the objective of protecting against intrusions, the physically secure environment will consist of:

    - Dedicated computing center with true floor to ceiling walls,
    - Physical security requiring two-person access, to gain access into the secure cabinet containing the Telstra RSS CA.

17. 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.

18. 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.

19. Entrance to the Computer Room will require the use of individual access proximity cards.
20. 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.

21. When a PIN or password is recorded, it shall be stored in a security container accessible only to authorized personnel.
22. 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.
23. 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.

5.1.2 Physical access

The TELSTRA RSS 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 RSA RSS CA is a locked enclosure with dual control authentication to which only PKI service operational authority personnel have physical access. The 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 RSS CA personnel with access to the physically secure environment must not have access to the VCR tapes or digital images. Procedures must exist for the granting and revocation of access privileges to individuals.

5.1.2.1.1 CA Physical Security Logs

24. Logs of access must be reviewed regularly and the review must be documented.
25. All access granting, revocation, and review procedures must be documented.
26. 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,
27. Visitors (contractors, maintenance personnel, etc.) to the CA facility are to be escorted by authorized individuals and sign an access logbook. This log must be maintained within the CA server room. This logbook must 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.
28. Significant alarm events must be documented. Under no circumstances shall an individual sign-off on an alarm event in which they were involved.
29. The use of any emergency entry or exit mechanism must cause an alarm event.
30. A process must exist for synchronizing the time and date stamps of the access, intrusion detection and monitoring (camera) systems to ensure accuracy of logs. This may be done by either automated or manual mechanisms. If a manual process is utilized, then the process must be performed at regular intervals to ensure accuracy.

5.1.2.1.2 Subscriber Physical Security Controls

Subscribers shall provide the necessary protection to their private keys when or when not in use. 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.

5.1.3 Power and air conditioning

The TELSTRA RSS CA must ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water exposures

The TELSTRA RSS CA must ensure that the CA system is protected from water exposure.

5.1.5 Fire prevention and protection

The TELSTRA RSS CA must ensure that the CA system is protected with a fire suppression system.

5.1.6 Media storage

The TELSTRA RSS CA must ensure that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

5.1.7 Waste disposal

The TELSTRA RSS CA must ensure sanitization or destruction of all sensitive or confidential data, storage media and computer equipment before release for disposal.

5.1.8 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.

5.2 Procedural controls

5.2.1 Trusted roles

The TELSTRA RSS CA shall require 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[1]. 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 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;

[1] 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".

- 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, revocation, etc (see Section 5.4.1).
- Technical controls that enforce dual access
- Policy and procedural controls that require dual access

5.2.1.1 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.

5.2.1.2 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.

5.2.1.3 CA 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.

5.2.1.4 Operating System Administrator

The operating system hosting the TELSTRA RSS 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.

5.2.2 Number of persons required per task

The TELSTRA RSS CA 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 RSS CA 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 the CA and activate a CA signing key.

Multi-user control is required for CA key generation as outlined in Section 6.2.2.

TELSTRA RSS 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.

5.2.3 Identification and authentication for each role

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

31. Included on the access list for the CA facility;
32. Included on the access list for physical access to the CA system;
33. 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.

5.2.4 Roles requiring separation of duties

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

5.3 Personnel controls

The TELSTRA RSS CA requires that all personnel performing duties with respect to the operation of a CA or who are stakeholders in the management of the CA shall:

34. Be appointed in writing;
35. Be bound by the terms and conditions of the role they are to fill;
36. Have received appropriate training with respect to the duties they are to perform;
37. Be bound not to disclose sensitive CA security-relevant information or Subscriber information; and
38. Not be assigned duties that may cause conflict with their CA duties.

5.3.1 Qualifications, experience, and clearance requirements

The TELSTRA RSS CA requires that all personnel performing duties with respect to the operation of a CA 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.

5.3.2 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;

5.3.3 Training requirements

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

- IT Security and General PKI knowledge;
- CA administration and operation; and
- CA disaster recovery processes.

5.3.4 Retraining frequency and requirements

The requirements for Section 5.3.3 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.

5.3.5 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.

5.3.6 Sanctions for unauthorized actions

All employees of the TELSTRA RSS 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 RSS 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 RSS CA, Telstra Corporation PKI Governance Council will suspend the person's access to the TELSTRA RSS CA immediately until an investigation is conducted. At the discretion of Telstra Corporation PKI Governance Council and Telstra Corporation executives, further action may be recommended regarding employment status.

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

5.3.7 Independent contractor requirements

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.

5.3.8 Documentation supplied to personnel

The TELSTRA RSS CA will make available to its employees/contractors the RSA RSS CP, this CPS and any specific procedures, documents and contracts relevant to their position. This includes CA Operating Procedures, Subscriber Agreements, Disaster Recovery Plans, and any other document required by personnel to perform their duties.

5.4 Audit logging procedures

Audit log files are generated for all events relating to the security of the TELSTRA RSS 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 if required by law.

5.4.1 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 Center facility , computer room and CA enclosure access;
- Logical events such as operating system operations and CA system operations.

Physical events may use electronic recording and/or logbooks.

Logical events will be recorded automatically in audit logs at the operating level and application level.

5.4.1.1 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.

5.4.1.2 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 should be digitally signed to maintain integrity of the information.

5.4.1.2.1 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

5.4.1.2.2 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

5.4.1.3 Consolidation requirements

Information pertaining to the TELSTRA RSS 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**.**

5.4.2 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.

Audit log data will be archived every 6 months

5.4.3 Retention period for audit log

The TELSTRA RSS 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 Section 5.5.2.

5.4.4 Protection of audit log

TELSTRA RSS 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 RSS 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.

5.4.5 Audit log backup procedures

Audit logs and audit summaries shall be backed up or copied (component backups and system backups), as described in the Disaster Recovery Plan and/or CA Operating Procedures, and placed in a secure area.

5.4.6 Audit collection system (internal vs. external)

The TELSTRA RSS 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 startup, and cease only at operating system shutdown. CA System audit processes will be invoked at CA application startup 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 RSS CA shall determine whether to suspend CA operations until the problem is remedied.

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

5.4.7 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.

5.4.8 Vulnerability assessments

Events in the audit process are logged, in part, to monitor inappropriate behavior, system vulnerabilities and/or compromises. TELSTRA RSS CA shall perform a vulnerability assessment, make appropriate recommendations to resolve issues and take appropriate action, as required, following an examination of these monitored events based on the frequency defined in Section 5.4.2.

5.5 Records archival

5.5.1 Types of records archived

TELSTRA RSS 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 RSS 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

5.5.2 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 RSS CA.

5.5.3 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 RSS 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 RSS 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.

5.5.4 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.

5.5.5 Requirements for time-stamping of records

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

5.5.6 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.

5.5.7 Procedures to obtain and verify archive information

TELSTRA RSS 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.

5.6 Key changeover

TELSTRA RSS CA key changeover is based on contractual obligations. If a new TELSTRA RSS CA key changeover is required (e.g., due to expiration), the CA shall generate a new key pair and submit the certificate to the RSA ROOT SIGNING SERVICE for signature. The old CA key pair shall be removed once no longer required for operation from the CA and destroyed. There shall be a key changeover period where the TELSTRA RSS CA phases out the previous CA private key and public certificate. The TELSTRA RSS CA private key shall not be used to sign issued certificates with a lifetime greater that the lifetime of the TELSTRA RSS 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.

Subscribers without valid key pairs must be re-authenticated in accordance with procedures in Section 3.2. When a Subscriber's certificate has been revoked as a result of non-compliance with TELSTRA RSS CA CPS or Subscriber agreement, the TELSTRA RSS CA must verify that the reasons for non-compliance have been addressed to the CAs satisfaction prior to certificate re-issuance.

5.7 Compromise and disaster recovery

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

5.7.1 Incident and compromise handling procedures

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

5.7.2 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.

5.7.3 Entity private key compromise procedures

In the unlikely event of the compromise of the private key associated with the TELSTRA RSS CA certificates the following steps shall be taken:

- The RSA ROOT SIGNING SERVICE shall be notified as soon as practicable;
- All subscribers shall be notified as soon as practicable; and
- Further action determined by the RSA ROOT SIGNING SERVICE shall be implemented.

Subscriber key compromise will result in immediate revocation. Re-issuance will be in accordance with section 3.3.2.

5.7.4 Business continuity capabilities after a disaster

A CA shall provide 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.

5.8 CA or RA termination

In the event that TELSTRA RSS 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 as stipulated in Section 5.5.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

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 6.1.6.

6.1.2 Private Key delivery to subscriber

The private and public key pair generated by the TELSTRA RSS CA 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.

6.1.3 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.

6.1.4 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 RSS CA public keys (as part of its certificate), and associated root certificate chain to the RSA Root Signing 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 RSA ROOT SIGNING SERVICE is signed by the RSA Security 2048 V3 CA, that is pre-installed in common web browser and web server software by the software manufacturer.

6.1.5 Key sizes

The Telstra RSS Policy CA will use the RSA cryptography key algorithm with a minimum key length of 2048 bits.

The Telstra Intermediate 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 1024 bits.

6.1.6 Public key parameters generation and quality checking

6.1.6.1 CA key generation

TELSTRA RSS 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.

6.1.6.2 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).

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

See section 7 for key usage as per Section 7.1.1 base certificates and 7.1.2 certificate extensions.

The Telstra Issuing CA private key will be used only for signing end entity certificates and CRLs. The key usage will be set for key certificate signing and CRL signing.

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.

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’.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

CA Keys are to be 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.

6.2.1 Cryptographic module standards and controls

The TELSTRA RSS 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. There is no requirement for any HSMs to be run in ‘FIPS mode’ within the TELSTRA RSS CA or web server SSL crypto accelerators.

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

There shall be multiple person control for CA key generation operations. At a minimum, there shall be 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 5.2.2 shall be applied.

6.2.3 Private Key escrow

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 application server, device and web server SSL private keys.

6.2.4 Private Key backup

The TELSTRA RSS CA will back up CA private signing keys in a secure manner to support disaster recovery operations and as detailed in the TELSTRA RSS 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).

6.2.5 Private Key archival

The TELSTRA RSS CA private signing key will not be archived.

6.2.6 Private Key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private Key storage on cryptographic module

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

6.2.8 Method of activating private key

Entities must be authenticated to the cryptographic module before the activation of the protected private key. This authentication, at a minimum will be in the form of a password. When deactivated, private keys must be kept in encrypted form only.

6.2.9 Method of deactivating private key

When keys are deactivated the application must clear the keys 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 must automatically deactivate the private key after a pre-set period of inactivity.

6.2.10 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.

6.2.11 Cryptographic Module Rating

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

6.3 Other aspects of key pair management

6.3.1 Public key archival

The TELSTRA RSS 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 RSS CA shall retain all verification public keys for 7 years.

6.3.2 Certificate operational periods and key pair usage periods

Telstra RSS Policy CA and Telstra Issuing CA have key usage periods of eight (8) and five (5) years respectively, as stipulated in the **RSA ROOT SIGNING AGREEMENT** with RSA Security Inc.

Telstra end entity (end users, device and SSL) certificates will be issued with a validity period of no more than two (3) years. Subscriber key usage periods will be less than or equal to the remaining validity period of the TELSTRA RSS CA certificate remaining validity period.

6.4 Activation data

6.4.1 Activation data generation and installation

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

6.4.2 Activation data protection

All pass phrases are known to all current staff members of the 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.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The following functionality, for the TELSTRA RSS 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 RSS CA server shall include the following functionality:

39. Access control to CA services and PKI roles;
40. Enforced separation of duties for PKI roles;
41. Identification and authentication of PKI roles and associated identities
42. Use of cryptography for session communication and database security, mutually authenticated and encrypted sessions are used for all external communications;
43. Archival of CA and end entity history and audit data;
44. Audit of security related events;
45. Trusted path for identification of PKI roles and associated identities, use of X.509 certificates for all CA administrators; and
46. Recovery mechanisms for keys and CA system.

6.5.2 Computer security rating

No stipulation

6.6 Life cycle technical controls

6.6.1 System development controls

TELSTRA RSS 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.

6.6.2 Security management controls

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

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

The TELSTRA RSS CA shall have 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 RSS CA configuration management plan is detailed in the TELSTRA RSS CA Operating Procedures.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

The TELSTRA RSS CA server will be protected by appropriate network security controls. Network security controls will permit only authorized access to the TELSTRA RSS CA servers. Auditing will be enabled and checked on a frequent basis. Remote access to the TELSTRA RSS CA environment will be protected by authenticated encrypted 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.

6.8 Time-stamping

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

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

TELSTRA RSS CA shall issue X.509 Version 3 certificates, in accordance with the PKIX Certificate and CRL Profile.

7.1.1.1 Base certificate format

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

7.1.2 Certificate extensions

7.1.2.1 CA Certificates

The TELSTRA RSS 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 RSS 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=1.2.840.113549.5.6.1)
CRL Distribution Point	No	Empty
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=1.2.840.113549.5.6.1)
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

7.1.2.2 Application Server Certificates

The TELSTRA RSS 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=1.2.840.113549.5.6.1)
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	RSS Live Comms Server

7.1.2.3 OCSP Response Signing Certificates

The TELSTRA RSS CA will support the following extensions for OCSP Response Signing certificates:

Field	Criticality	Description
id-pkix-ocsp-nocheck (the object identifier 1.3.6.1.5.5.7.48.1.5)	Yes	NULL
Extended Key Usage	Yes	id-kp-OCSPSigning (labeled 1.3.6.1.5.5.7.3.9)

7.1.2.4 Individual Certificates

The TELSTRA RSS 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=1.2.840.113549.5.6.1)
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	RSS Email Signature Only

The TELSTRA RSS 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=1.2.840.113549.5.6.1)
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	RSS Email Encryption

7.1.3 Algorithm object identifiers

TELSTRA RSS CA shall use and Subscribers shall support, for signing and verification, the following:

50. RSA 1024 algorithm in accordance with PKCS#1; and/or
51. SHA-1 algorithm in accordance with FIPS PUB 180-1 and ANSI X9.30 part2; and/or
52. Additional algorithms as supported by the CA software and implemented Hardware Security Module.

7.1.4 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.

7.1.5 Name constraints

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

7.1.6 Certificate policy object identifier

Certificate Policy extension will be used. The Object Identifier (OID) for the Certificate Policy corresponding to the appropriate certificate will be as set forth in this CPS.

7.1.7 Usage of Policy Constraints extension

The TELSTRA RSS CA supports the use of the Policy Constraints extension.

7.1.8 Policy qualifiers syntax and semantics

TELSTRA RSS 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 RSS CA CPS. In addition, some Certificates contain a User Notice Qualifier which may point to an applicable Relying Party Agreement.

7.1.9 Processing semantics for the critical Certificate Policies extension

Critical extensions, when applicable, shall be interpreted as defined in PKIX.

7.2 CRL profile

7.2.1 Version number(s)

TELSTRA RSS 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

7.2.2 CRL and CRL entry extensions

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

The TELSTRA RSS 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.

7.3 OCSP profile

TELSTRA RSS CA shall provide OCSP service in accordance with the RFC 2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP" dated June 1999.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

A Compliance Audit provides an independent third party attestation that the TELSTRA RSS CA is operating as stated in the RSA RSS CP and this CPS. The TELSTRA RSS CA must have a Compliance Audit performed at their expense to demonstrate compliance with the RSA RSS CP.

8.1 Frequency or circumstances of assessment

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 contract to use the RSA ROOT SIGNING SERVICE.

The annual compliance audit will determine whether the TELSTRA RSS CA functioning (business practices and controls) meets the requirements of the RSA RSS CP, and this CPS.

8.2 Identity/qualifications of assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with requirements which the RSA ROOT SIGNING SERVICE 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.

8.3 Assessor's relationship to assessed entity

For both the RSA ROOT SIGNING SERVICE and TELSTRA RSS CA, the Compliance Auditor either shall be a private firm, which is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation and attestation. The RSA ROOT SIGNING SERVICE shall determine whether a Compliance Auditor meets this requirement.

8.4 Topics covered by assessment

The purpose of a yearly compliance audit shall be to verify that an entity is subject to the requirements of the RSA RSS CP and this CPS and, is complying with the requirements of those documents. The Compliance Audit will cover all requirements such as:

53. TELSTRA RSS CA business practices disclosure;
54. Service integrity (including key and certificate life cycle management activities);
55. TELSTRA RSS CA environmental controls.

8.5 Actions taken as a result of deficiency

When the Compliance Auditor finds a discrepancy between how the TELSTRA RSS CA is designed, being operated or maintained, and the requirements of this CPS and the RSA RSS CP, 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 RSS 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, RSA Security Inc. 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, RSA Security Inc. believes that the TELSTRA RSS CA is not in compliance with the RSA RSS CP, the RSA ROOT SIGNING SERVICE may, at its discretion, revoke the certificate of the TELSTRA RSS CA, depending on the severity of the non-compliance.

8.6 Communication of results

The Compliance Auditor will produce a Compliance Audit Report. The compliance audit report will be used by the TELSTRA RSS CA to demonstrate a good standing in its practices and procedures The Compliance Audit Report will be released to the RSA ROOT SIGNING SERVICE meeting the annual compliance audit requirement. All audit reports to include any corrective action taken will remain the sole property of TELSTRA RSS 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.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No fees will be charged unless otherwise stated in the CP under which the Certificates are issued.

9.1.2 Certificate access fees

No fees will be charged unless otherwise stated in the CP under which the Certificates are issued.

9.1.3 Revocation or status information access fees

No fees will be charged unless otherwise stated in the CP under which the Certificates are issued.

9.1.4 Fees for other services

Unless otherwise stated in the CP under which the Certificates are issued, TELSTRA RSS CA shall be responsible for all administrative expenses associated with the operation the TELSTRA RSS CA, including its costs of a Compliance Audit undertaken under section 8 of this document.

9.1.5 Refund policy

No refund will be made unless otherwise stated in the CP under which the Certificates are issued.

9.2 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.

9.2.1 Insurance coverage

TELSTRA RSS 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.

9.2.2 Other assets

Other assets are not addressed under this CPS.

9.2.3 Insurance or warranty coverage for end-entities

No warranty coverage is made available to Subscribers or Relying Parties under this CPS.

9.2.4 Relationship

Nothing in this CPS makes either TELSTRA RSS CA nor the Subscriber a trustee, principal, agent, fiduciary, or representative of the other. TELSTRA RSS CA makes no express or implied representation to the contrary. The Subscriber does not have any authority to bind TELSTRA RSS CA.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Subscriber information, not appearing in certificates and in public directories, held by TELSTRA RSS 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 RSS 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 RSS 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 RSS 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 9.3.1. Any request for the disclosure of information under paragraph (a) above shall be signed and delivered in writing to the TELSTRA RSS 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 RSS 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 9.3.1.

9.3.2 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:

56. 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;

57. Information that the receiving party lawfully receives from a source other than the disclosing party;

58. Information that is in or enters the public domain other than because of a breach by the receiving party of this CPS;

59. 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

60. Information that the disclosing party agrees in writing is not subject to an obligation of confidentiality.

9.3.3 Responsibility to protect confidential information

TELSTRA RSS CA must keep confidential information physically and/or logically protected from unauthorised viewing, modification or deletion. In addition, the CA must ensure that storage media

used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

9.4 Privacy of personal information

9.4.1 Privacy plan and laws

TELSTRA RSS 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.

9.4.2 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.

9.4.3 Information not deemed 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.

9.4.4 Responsibility to protect private information

TELSTRA RSS 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.

9.4.5 Notice and consent to use private information

Personal information will only be used, collected or disclosed consistently with section 9.4.1 and as may be required under section 9.4.6.

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

9.4.6 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.

9.4.7 Other information disclosure circumstances

Other requirements may apply as stated in the CP under which the Certificates are issued.

9.5 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 RSS 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 RSS CA CPS. Each of Telstra RSS 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 RSS CA and Telstra Corporation (as applicable) and remain free of any lien, charge, encumbrance or other third party interest.

9.6 Representations and warranties

TELSTRA RSS 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 3 and 4 of this CPS.

9.6.1 CA representations and warranties

TELSTRA RSS CA will conduct itself in accordance with the RSA RSS CP, this CPS and applicable laws, as described in section 9.14 and 9.15, when issuing and managing certificates provided to Subscribers. TELSTRA RSS 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 RSS CA is subject always to section 9.8.

When TELSTRA RSS 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 the RSA RSS CP and 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 RSS 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 RSS CA. TELSTRA RSS 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.

9.6.2 RA representations and warranties

All RAs performing Subscriber registration tasks on behalf of TELSTRA RSS CA must comply with all relevant provisions of RSA RSS CP, 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 RSS CA, in accordance with section 3.1 and section 4.1, for certificate requests and certificate revocation requests.

RAs shall be individually accountable for actions performed on behalf of TELSTRA RSS 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 RSS 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 3.1.

9.6.3 Subscriber representations and warranties

Subscribers registering and accepting a certificate from the TELSTRA RSS 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 enrollment page) shall be complete and validated and contains all information required in connection with a certificate request.

9.6.4 Relying party representations and warranties

Relying Parties acknowledge that it has read and accepts all terms and conditions of any associated Telstra service participation agreement.

9.6.5 Representations and warranties of other participants

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

9.7 Disclaimers of warranties

The TELSTRA RSS 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 RSS CA services are provided to end entities on an ‘as-is’ basis, without warranties of any kind, and TELSTRA RSS 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 RSS 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 RSS CA is limited, at its option, to:

a) In the case of services, the resupply of, or payment of the cost of resupplying, the service; and

b) In the case of goods:

    1. The replacement of the goods or the supply of equivalent goods;

    2. The repair of the goods;

    3. The payment of the cost of replacing the goods or of acquiring equivalent goods; or

c) The payment of the cost of having the goods repaired.

9.8 Limitations of liability

TELSTRA RSS 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 RSS CA service to materially comply with the terms and conditions of this CPS and/or applicable CP, and/or (2) a material breach of any express warranty made by the corporation in this CPS and/or applicable CP,

but only to the extent that such losses result from their reasonable use of a Certificate for transactions, applications, and purposes authorized in the applicable CP.

TELSTRA RSS 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 RSS 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 RSS 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 RSS 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 fulfill 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 RSS CA or to an RA by a person, organisation, or entity making application for issuance of a Certificate by the TELSTRA RSS 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 RSS CA service; or
- Due to disclosure of personal information contained within certificates and revocation lists.

TELSTRA RSS CA has no liability to the other party for or in respect of:

a) Any consequential, punitive, special or indirect liability, loss, damage or charge or any loss of profits, data, savings or income; or

b) 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 RSS CA has been advised of the likelihood or possibility of such liability.

9.9 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 RSS 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 RSS CA service, that arises from:

a) their failure to provide the 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 RSS 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 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 9.9. 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 CA.

9.10 Term and termination

9.10.1 Term

This CPS continues indefinitely until the earlier of:

(a) notice of termination or expiry provided by Telstra Corporation at TELSTRA RSS CA CPS' publishing point, at which time this CPS will immediately terminate; or

(b) the circumstances described in Section 9.10.2.

9.10.2 Automatic termination

This CPS will automatically terminate on publication of a newer version or replacement document by TELSTRA RSS CA (which document will, subject to Section 9.10.3, supersede this CPS), or upon TELSTRA RSS CA ceasing CA operations.

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this CPS will be communicated at TELSTRA RSS 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.

9.11 Individual notices and communications with participants

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

9.12 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 RSS CA contact as described in Section 1.5. Decisions with respect to the proposed changes are at the sole discretion of Telstra Corporation PKI Governance Council.

9.12.1 Procedure for amendment

An electronic copy of TELSTRA RSS CA CPS is to be made available at the Telstra web site http://pki.telstra.com.au/TelstraRSSCPS.pdf,or by requesting an electronic copy by e-mail to the contact representative as described in Section 1.5.

TELSTRA RSS 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.

9.12.2 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 RSS CA CPS publishing point.

The comment period will be 30 days unless otherwise specified. The comment period will be defined in the notification.

9.12.3 Circumstances under which OID must be changed

If a policy change is determined by RSA ROOT SIGNING SERVICE to warrant the issuance of a new policy, the RSA ROOT SIGNING SERVICE will assign a new Object Identifier (OID) for the new policy and notify the TELSTRA RSS CA.

9.13 Dispute resolution provisions

Any dispute related to Key and Certificate management between the TELSTRA RSS 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 RSS 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 9.13 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.

9.13.1 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.

9.13.2 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 9.13.1(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 9.13.3

9.13.3 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.

9.14 Governing law

The RSA RSS CP and all corresponding agreements shall be governed by the laws of Victoria, Australia.

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

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

9.16.2 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.

9.16.3 Force Majeure

TELSTRA RSS 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.

9.17 Other provisions

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

ABBREVIATIONS

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
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
RFC	Request For Comment
RSA	Rivest-Shamir-Adleman
SHA –1	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

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 enrollment, 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 enrollment process.

TERM: Administrator
DEFINITION: A Trusted Person within the organization of a Processing Center, Service Center, 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 through out 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 RSS 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 (NIST). 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: X501PrintableString
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