

TELSTRA RSS CA Subscriber Agreement (SA)

Last Revision Date: December 16, 2009

Version: 1.0

Published By: Telstra Corporation Ltd



Copyright © 2009 by Telstra Corporation

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without prior written permission of Telstra Corporation and RSA Security Inc.

REVISION HISTORY

Date	Author's Initials	Version	Author's Comments
15 July 2009	GD (Telstra)	0.0	First Draft
24 July 2009	GD, SA (Telstra)	0.1	Internal Review
10 Aug 2009	GD (Telstra)	0.2	Incorporated feedback
16 December 2009	VV, SA, CP (Telstra)	1.0	Alignment with CPS, general formatting upgrades and promoted to release 1.0

IMPORTANT NOTICE ABOUT THIS DOCUMENT

This communication does not substitute or replace the RSA RSS Certificate Policy under which digital certificates issued by this Issuing Authority are issued. You must read the [Certificate Policy](#) and the [Telstra RSS CA CPS](#) which ultimately controls the provision of digital certification services, before you apply for a certificate.

For your convenience, a quick summary of some important points of the Certificate Policy is set out in the form of a Subscriber Agreement.

You must read this Subscriber Agreement before applying for, accepting, or using a Telstra RSS Issuing CA Certificate. If you do not agree to the terms of this Subscriber Agreement, do not apply for, accept, or use the Digital Certificate. On enrolment for a Telstra RSS Issuing CA Digital Certificate, you will be asked to confirm that you have read and agree to the terms of this Subscriber Agreement.

By accepting or using a certificate, you agree to become a party to, and be bound by, the terms mentioned in this Subscriber Agreement.

TABLE OF CONTENTS

1. DEFINITIONS	5
2. PROCESSING THE CERTIFICATE APPLICATION.....	6
3. SUBSCRIBER OBLIGATIONS	6
4. REVOCATION	7
5. OBLIGATIONS UPON REVOCATION AND EXPIRATION	7
6. TERMS OF SERVICE	7
7. CHARGES AND PAYMENT TERMS	7
7.1 REFUND POLICY (IF ANY)	7
8. TELSTRA RSS ISSUING CA OBLIGATIONS	7

1. DEFINITIONS

TERM: Certification Authority

DEFINITION: Certification Authority or CA means an entity authorised to issue, suspend, or revoke certificates. For purposes of this Agreement, CA shall mean Telstra RSS Issuing Certification Authority.

TERM: Certificate Application

DEFINITION: Certificate Application means a request to a CA for the issuance of a Certificate.

TERM: Certification Practice Statement

DEFINITION: Certification Practice Statement or CPS means 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. this document is revised from time to time, representing a statement of the practices a CA employs in issuing Certificates. Telstra RSS CA's CPS is published at http://telstra-pki.telstra.com.au/Telstra_RSS_CPS.pdf.

TERM: Common Name

DEFINITION: Common Name or CN is typically composed of Host + Domain Name and will look like "www.yoursite.com" or "yoursite.com". In case of individual certificates "Common Name" refers to the name of the individual.

TERM: Certificate Revocation List

DEFINITION: Certificate Revocation List or CRL means 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: Digital Certificate

DEFINITION: Digital Certificate means a digitally signed electronic data file (conforming to the X509 version 3 ITU standard) issued by Telstra RSS Issuing CA in order to identify a person or entity seeking to conduct business over a communications network using a Digital Signature and which contains the identity of the person authorised to use the Digital Signature and a copy of their Public Key, a serial number, a time period during which the Digital Certificate may be used.

TERM: Registration Authority

DEFINITION: Registration Authority or RA shall mean an individual and/or entity approved by Telstra RSS Issuing CA to perform Authentication, assist Subscribers in applying for Certificates, verification of certificate request content (applicant information) on behalf of a CA, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.

TERM: Relying Party

DEFINITION: Relying Party means an individual or organization that acts in reliance on a Certificate and/or a digital signature. All Relying Parties entrusted with a certificate issued by The TELSTRA RSS ISSUING CA must abide by the provisions of this CPS.

TERM: Relying Party Agreement

DEFINITION: Relying Party Agreement means an agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party, such as the [Telstra RSS Issuing CA Relying Party Agreement](#).

TERM: Repository

DEFINITION: Repository means 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 from one or more CAs and makes them available to entities that need them for implementing security services.

TERM: RSA RSS

DEFINITION: RSA RSS refers to RSA Inc.'s Root Signing Services.

TERM: Subscriber

DEFINITION: Subscriber is an entity, a person or application server that is a holder of a private key corresponding to a public key and has been issued a certificate by Telstra RSS CA. In case of an application server, a person authorized by the organization owning the application server may be referred to as the subscriber.

2. PROCESSING THE CERTIFICATE APPLICATION

Upon receipt of the necessary payment (where ever applicable), completion of authentication procedures required for the Certificate you have selected and upon receipt of all the technical requirements for the certificate you have selected, Telstra RSS Issuing CA will process your Certificate Application. If your Certificate Application is approved, Telstra RSS Issuing CA will issue you a Certificate for your use in accordance with this Subscriber Agreement. After you pick up or otherwise install your Certificate, you must review the information in it and promptly notify Telstra RSS Issuing CA of any errors. Upon receipt of such notice, Telstra RSS Issuing CA may revoke your Certificate and issue you a corrected Certificate.

3. SUBSCRIBER OBLIGATIONS

This Subscriber Agreement will become effective on enrolling for a certificate from the Telstra RSS CA.

- By accepting this Subscriber Agreement (and submitting information requested in the enrolment forms), I am requesting that the Issuing Authority issue a digital certificate to me and am expressing my agreement to the terms of this subscriber agreement. I understand that RSA Root Signing (RSS) Service Certification Services are governed by the Certificate Policy at [Certificate Policy](#) as may be amended from time to time, and which is incorporated by reference into this subscriber agreement.
- I agree to use the digital certificate and any related Digital Certification Services in accordance with the Certificate Policy and only in relation to usages authorised by [Telstra RSS CA CPS](#). By applying for a certificate, I confirm that I have read the Certificate Policy and Certification Practice Statement and agree to all its terms.
- I agree that any passwords, pass-phrases, PINs, private keys or other personal secrets used in obtaining authenticated access to PKI facilities must remain confidential to me only. I agree to protect such information from access by anyone or anything other than me until it is securely destroyed and certify that no unauthorised person has ever had access to such secret information that I may use as part of the application for a certificate. I acknowledge that the Issuing Authority has provided me with sufficient information to become familiar with the use of my certificate before applying for, using and relying upon a certificate.
- I agree to immediately inform the Telstra RSS Issuing CA or its nominated representative, should any passwords, pass-phrases, PINs, private keys or other personal secrets used in obtaining authenticated access to PKI facilities, be compromised or be suspected of being compromised.
- I certify that all information provided by myself in support of an application for a digital certificate is true to the best of my knowledge.
- I acknowledge that certain information provided by me at the time of enrolment will be embedded in a digital certificate, and may be published in a directory of certificates and revocation information where required for the purpose of operating the digital certification services. I consent to the disclosure of this information for these purposes and understand that I have the right to correct any information about me.
- I understand that further information on my rights in this respect is to be found in the Privacy Charter, located at http://www.telstra.com.au/privacy/privacy_telstra.html

4. REVOCATION

If you discover or have reason to believe there has been a compromise of your private key, or the information within your Certificate is incorrect or has changed, or domain name registration has changed, you must immediately notify Telstra RSS CA. Telstra RSS Issuing CA retains the right to revoke your Certificate at any time without notice if:

- Telstra RSS Issuing CA discovers that the information within your Certificate is no longer valid;
- Or, you fail to comply with obligations set out in the RSA RSS CP, this CPS, Subscriber agreement or applicable law;

5. OBLIGATIONS UPON REVOCATION AND EXPIRATION

Upon expiration or notice of revocation of your Certificate, you shall permanently remove your Certificate from all devices on which it is installed and shall not use it for any purpose thereafter.

6. TERMS OF SERVICE

This Agreement shall remain in effect until your Certificate has expired or is revoked (whichever is earlier).

7. CHARGES AND PAYMENT TERMS

7.1 Refund policy (if any)

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

8. TELSTRA RSS ISSUING CA OBLIGATIONS

Telstra RSS Issuing CA will:

- Comply with the conditions and obligations set out in the RSA RSS CP and the practices set out in the [Telstra RSS CA CPS](#);
- Generate Certificates only on the receipt of properly formatted and verified Certificate requests;
- Make and receive revocation requests and take appropriate action;
- Issue a new Certificate to a Certificate Holder that suspects its Keys or Certificates have or may have become compromised or after receiving a properly formatted and verified request from the relevant Certificate Holder or Authorised Officer for a new Certificate;
- Ensure a copy of the relevant RSA RSS CP and the [Telstra RSS CA CPS](#) is made accessible to each Subscriber;
- Correctly identify individuals requesting, or ensure procedures for identifying individuals have been followed by parties requesting certificates;
- Ensure that Private Keys and key transport access control mechanisms are not obtained by third parties prior to being received by a Certificate Holder.