

# **TELSTRA RSS CA Relying Party Agreement (RPA)**

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**

<b>Date</b>	<b>Author's Initials</b>	<b>Version</b>	<b>Author's Comments</b>
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 Dec 2009	VV, SA (Telstra)	1.0	Alignment with CPS

## **IMPORTANT NOTICE ABOUT THIS DOCUMENT**

You must read this relying party agreement before validating a Telstra RSS Issuing CA Certificate, using Telstra RSS CA's Online Certificate Status Protocol services, accessing or using a Telstra RSS Issuing CA Database of Certificate Revocations. If you do not agree to the terms of this relying party agreement, you are not authorised to use the repository or rely on a certificate issued by the Telstra RSS CA. In consideration of your agreement to these terms, you are entitled to use the Telstra RSS Issuing CA information as set forth herein.

## TABLE OF CONTENTS

1. DEFINITIONS .....	5
2. TERMS OF AGREEMENT .....	6
3. INFORMED DECISION .....	6
4. CERTIFICATES .....	6
5. RELYING PARTY OBLIGATIONS .....	6
6. LIMITATIONS OF USE .....	6
7. TELSTRA RSS ISSUING CA WARRANTIES.....	7
8. DISCLAIMERS OF WARRANTIES .....	7
9. FORCE MAJEURE .....	8
10.GOVERNING LAW AND DISPUTE RESOLUTION .....	8
11.NOTICES.....	9
12.ENTIRE AGREEMENT.....	9

## 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](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. TERMS OF AGREEMENT

This Agreement becomes effective when you submit a query to search for a Telstra RSS Issuing CA Certificate, or rely on any Telstra RSS Issuing CA Information. This Agreement shall be applicable for as long as you use a Telstra RSS Issuing CA certificate or rely on any Telstra RSS Issuing CA Information.

## 3. INFORMED DECISION

You acknowledge and agree that:

- You have sufficient information to make an informed decision as to the extent to which you choose to rely on the information in a Certificate;
- Your use of or reliance on any Telstra RSS Issuing CA Information is governed by this Agreement and you shall bear the legal consequences of your failure to comply with the obligations contained herein. YOU ARE SOLELY RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON THE INFORMATION IN A CERTIFICATE.

## 4. CERTIFICATES

Telstra RSS Issuing CA offers different types of certificate services as highlighted in the [Telstra RSS Issuing CA Certification Practice Statement](#), with each type providing specific functionality and security features corresponding to a specific level of trust within the RSA Root Signing Service (as highlighted in the RSA Root Signing Service Certificate Policy).

## 5. RELYING PARTY OBLIGATIONS

As a Relying Party, you are obligated to ensure the reasonableness of your reliance on any Telstra RSS Issuing CA Information by:

- Assessing whether the use of a Certificate for any given purpose is appropriate under the circumstances;
- Utilizing the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations you wish to perform, as a condition of relying on a Certificate in connection with each such operation;
- Checking the status of a Certificate you wish to rely on, as well as the validity of all the Certificates in its chain.

## 6. LIMITATIONS OF USE

TELSTRA RSS ISSUING 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 ISSUING 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 authorized by TELSTRA RSS ISSUING 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 unauthorized use of one or more private Keys;
- Arising from the provision of any information to TELSTRA RSS ISSUING CA or to an RA by a person, organization, or entity making application for issuance of a Certificate by the TELSTRA RSS ISSUING 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 ISSUING CA service; or
- Due to disclosure of personal information contained within certificates and revocation lists.

In no event will Telstra RSS Issuing CA be liable for incidental, any consequential, punitive, special or indirect liability, loss, damage or charge or any loss of profits, data, savings or income; or loss, damage or destruction of data, regardless of the form of action, whether in contract, tort (including negligence), breach of warranty or otherwise, 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 Issuing CA has been advised of the possibility of the same. No limitation as to damages for personal injury is hereby intended.

## 7. TELSTRA RSS ISSUING CA WARRANTIES

TELSTRA RSS ISSUING CA will conduct itself in accordance with the RSA RSS CP, this CPS and applicable laws. When issuing and managing certificates provided to Subscribers. TELSTRA RSS ISSUING 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 ISSUING CA is subject always to Limitations of liability of Telstra RSA CA CPS.

When TELSTRA RSS ISSUING 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 [Telstra RSA CA 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 [Telstra RSA CA 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 ISSUING 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.

## 8. DISCLAIMERS OF WARRANTIES

The Telstra RSS Issuing CA Issuing Authority's liability to you is limited to that specified in RSA RSS Certificate Policy.

The TELSTRA RSS ISSUING 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 ISSUING CA services are provided to end entities on an 'as-is' basis, without warranties of any kind, and TELSTRA RSS ISSUING 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 ISSUING 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 ISSUING 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:
  - I. the replacement of the goods or the supply of equivalent goods;
  - II. the repair of the goods;
  - III. the payment of the cost of replacing the goods or of acquiring equivalent goods;  
or
  - IV. The payment of the cost of having the goods repaired.

## 9. FORCE MAJEURE

TELSTRA RSS ISSUING 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.

## 10. GOVERNING LAW AND DISPUTE RESOLUTION

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

### 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) of Telstra RSA CA CPS, 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 organization other than the ACDC, in which case the mediation is to be conducted in accordance with the current guidelines of that organization (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 administered 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 of Telstra RSA CA CPS.

## **11. NOTICES**

You will make all notices, demands or requests to Telstra Corporation Limited with respect to this Agreement in writing to:

Telstra Corporation Limited  
Information Security Operations Manager  
242 Exhibition St  
Melbourne Victoria 3000 Australia  
Email: [pki.operations@team.telstra.com](mailto:pki.operations@team.telstra.com)

## **12. ENTIRE AGREEMENT**

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