Controlling Document

Telstra Hosted CBA CA Certificate Policy

Published By: Telstra PKI Team

Last Updated: 5th December 2024

Telstra Corporation Limited
ABN 33 051 775 556

Telstra Corporation Limited PKI Certificate Policy

Trademark Notices

Telstra is the registered trademark of Telstra Corporation Limited. The Telstra logo, Telstra Network and BigPond are trademarks and service marks of Telstra Corporation Limited, Inc. Other trademarks and service marks in this document are the property of their respective owners. Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of Telstra Corporation Limited. Notwithstanding the above, permission is granted to reproduce and distribute these Telstra Corporation Limited Certificate Policies on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to Telstra Corporation Limited, Requests for any other permission to reproduce these Telstra Certificate Policies (as well as requests for copies from Telstra) must be addressed to Telstra, Telstra PKI Policy Management Authority.

REVISION HISTORY

Version	Date	Detail	Author	Status
1.2.1	05 December 2024	Final publication for 4th DEC 2024 Telstra Purple hosted CBA Root CA	PKI Team	Published
1.2	04 December 2024	Final publication for 4th DEC 2024 Telstra Root CAs	PKI Team	Published
1.1	October 2024	Publication for AD root	PKI Team	Published
1.0	September 2024	Baseline CP	PKI Team	Published

Table of Contents

1. Introduction

1.1. Purpose

PKI digital certificate and its associated certificate policies (CP) play critical roles in the administration of authenticate and/or encrypt communications over private network or public Internet. The main purpose of a PKI CP is to enable relying party to determine whether the certificate with the binding public key and the underlying conditions are sufficiently "trustworthy" and accurate for a given interaction. Equally, certificate subject or subscriber has clear guidance upon which they can use their corresponding private key to sign and/or encrypt a piece of information, and place reliance on the certification service to support it.

This document provides high level certificate policy requirements for Telstra hosted CBA RSA4096 SHA256 Root CA to ensure that Telstra PKI service provides Confidentiality, Integrity, Authenticity and Non-repudiation digital certificate and other relevant PKI services. This document is for Telstra hosted CBA RSA4096 SHA256 Root CA digital certificates that adopted the X.509 version 3 format as outlined in RFC 3647, and the principles and practices related to the Telstra PKI service digital certificate certification of non-cross-certified and non-publicly trusted digital certificates.

This certificate policy (CP) includes the following distinct certificate policies:

- A policy for devices with software cryptographic modules, and
- A policy for devices with hardware cryptographic modules.

In this document, the term "device" refers to a non-person entity, i.e., a hardware device or software application.

This certificate policy document shall be interpreted in accordance with the up-to-date Telstra CA Certification Practice Statement (CPS), Telstra Cryptography Standard, Telstra Data Protection Standard and other relevant Telstra PKI and Telstra security documentation (please see appendix for reference details).

1.2. Scope

As Telstra PKI currently offer low assurance level certificate, this CP indicate the applicability of a certificate to Telstra hosted CBA RSA4096 SHA256 Root CA with common security requirements.

1.3. Document Identification

The commencement date of this CP is: 5th December 2024. This CP references the Telstra hosted CBA RSA4096 SHA256 Root CA CPS. The OID for the Telstra Hosted CBA RSA4096 SHA256 Root CA CPS = 1.3.6.1.4.1.1088.4.27.5.2.3

1.4. Relationship Between CP & CPS

A Certificate Policy (CP) is a set of rules that indicates the applicability of a certificate to Telstra enterprise community and/or Telstra applications (and/or Telstra hosted applications, e.g, CBA) with common security requirements. A CP may be used by a relying party to help in deciding whether a certificate, the binding of the public key are trustworthy and otherwise appropriate for a particular application (*i.e., use case*). A Certification Practice Statement (CPS) is a more detailed description of the practice followed by a CA in issuing certificates.

This CP states the requirements for the issuance and management of certificates issued by Telstra CAs, and requirements for the operation of these CAs. The CPS states how the Telstra CAs implement the requirements. Each CA that issues certificates under a CP must have a corresponding approved Telstra CPS.

The CP or CPS has no contractual significance hence the CPs and CPSs are strictly informational and disclosure documents.

1.5. Publication and Repository Responsibility

Telstra hosted CBA RSA4096 SHA256 Root CA CP and CPS are published at*:* telstra-pki.pki.telstra.com.au/cps/. It is expected that this document will be revisited and revised from time to time to ensure its continued reliability as an operational requirement for Telstra CAs.

Telstra MAY publish additional CPs or CPSs to applicable Telstra users or relying parties, as necessary, to describe other PKI service offerings and to provide a comprehensive Telstra PKI governance framework. Other potential documents may include Telstra Cryptographic Key Management Plan and Policies, Telstra PKI Registration Authority Agreements, Registration Authority Practices Statement (RPS), Telstra PKI Relying Party Agreements, Telstra PKI Subscriber Agreement.

2. Identification and Authentication

Below detailed section proposes the generic CP reference to the Telstra hosted CBA RSA4096 SHA256 Root CA and the CBA issuing CA CBNSTL5GFCA01 which is managed by Telstra Purple CBA team.

2.1. Naming

An entity in PKI context is also known as a “subject”, including an individual, organisation, account and/or device. This CP only consider the device as the “subject”, such as Telstra hosted application server managed by the Telstra Purple CBA team. The subject will use Common Name (CN) as the certificate’s entity name. In other situation, a Subject Alternative Name (SAN) is also used, it structures and lists all the domain names and IP addresses that fall under the security umbrella of a particular certificate. SAN define a particular DNS amongst the other servers hosted on the same server, e.g., subdomains.

2.2. Identification

In general, the PKI identification involves two generic processes:

(1) Establishing that a given name of an individual or organisation corresponds to a real-world identity of an individual or organisation, and

(2) Establishing that an individual or organisation applying for or seeking access to something under that name is, in fact, the named individual or organisation.

The first process is also commonly known as “identification”, with the 2nd process as “Authentication”, please refer to Section 2.3.

2.3. Authentication

Authentication - establishing the user, team and application applying for a certificate is, in fact, the user or application they claimed to be. This process corresponds to the above identification process.

2.4. Identification and Authentication for Revocation Request

Managed by Telstra Purple CBA team.

2.5. Identification and Authentication for Key Recovery Request

Managed by Telstra Purple CBA team.

3. Telstra Hosted CBA RSA4096 SHA256 Root CA and Certificate Policy

Telstra CBA RSA4096 SHA256 Root CA hosted by Telstra PKI operation team. The hosted CBA issuing CA CBNSTL5GFCA01 is managed by Telstra Purple CBA team. Below detailed section proposes the generic CP reference to the hosted CBA issuing CA CBNSTL5GFCA01.

3.1. High Level Requirements

1. Certificate requests shall be accurate, authenticated and approved in accordance with the applicable CP or CPS.
2. Certificate renewal requests shall be accurate, authorised, and complete in accordance with the applicable CP or CPS.
3. New and renewed certificates shall be generated and issued in accordance with the applicable CP or CPS.

3.2. Certificate Management Process

Managed by Telstra Purple CBA team.

3.3. Certificate Registration and Issuance

1. The issuing CA or the RA (Dcerts) shall verify or require the credentials presented by a subject (subscriber and/or certificate applicant) as evidence of identity or authority to perform a specific role in accordance with the certificate policy.
2. Identification and authentication of a subject (subscriber and/or certificate applicant) shall precede any other processes (e.g. certificate issuance) in connection with the subject in question as required by this CP.
3. Issuing CA shall verify the accuracy of the information included in the requesting entity’s certificate request in accordance with the CP.
4. The issuing CA shall check the certificate request for errors or omissions in accordance with the CP.
5. For end entity certificates, the issuing CA shall ensure that the signing request is securely submitted and is authenticated as coming from an authorised entity.
6. Encryption and access controls shall be used to protect the confidentiality and integrity of registration data in transit and in storage.
7. At the point of registration (before certificate issuance) the issuing CA shall inform the subject or, where applicable, the subscriber of the agreements regarding use of the certificate.
8. A record of registration and related administrative data presented by a subject as evidence of identity shall be kept by the issuing CA and/or RA.
9. The issuing CA shall require that an entity requesting a certificate shall prepare and submit the appropriate certificate request data (registration request) to Issuing CA and/or the RA as specified in the CP.
10. There shall be evidence of the subjects’ agreement to the terms and conditions.
11. The issuing CA and/or the RA shall record the success or failure of the registration event in an audit log.
12. The Issuing CA and/or the RA shall store the certificate enrolment data in a database which is protected against unauthorized access, alteration, and deletion.
13. The Issuing CA and/or the RA shall ensure that the 'Identification and registration' process is secure. In particular every transfer of registration and identification inside or outside the Issuing CA or the RA shall be protected against eavesdropping and manipulation.

3.4. Certificate Deployment (Acceptance)

1. The issuing CA shall make the certificates available to relevant parties using an established mechanism (e.g. a repository such as a directory) in accordance with the CP. Possible mechanisms include:
   a) collection – repository or online directory service;
   b) delivery – distributed using protected media (e.g. Encrypted USB).
2. Only authorised CA personnel shall administer the issuing CA's repository or alternative distribution mechanism.
3. The performance of the issuing CA's repository or alternative distribution mechanism shall be monitored and managed.
4. Where required, certificates shall be made available for retrieval only in those cases for which the subject's consent is obtained. If the CP requires that all certificates issued by this CA are made available, the issuing CA shall not issue a certificate for a subject unless that subject's consent for such distribution is obtained.

3.5. Key Pair and Certificate Usage

1. The activation of the CA private signing key shall be performed using at least dual control, by person(s) in a trusted role. It is recommended to use multi-party control (i.e. m of n where n > m).
2. Based on a risk assessment, the activation of the CA private key should be performed using multifactor authentication (e.g. hardware token and password, biometric and password).
3. CA signing key(s) used for generating certificates or issuing revocation status information, shall not be used for any other purpose.
4. The CA's private keys shall only be used within physically secure premises
5. The CA shall cease to use a key pair at the end of the key pair's defined operational lifetime or when the compromise of the private key is known or suspected.
6. Correct processing of CA cryptographic hardware should be verified on a periodic basis.
7. An annual review should be required by the PA on key lengths to determine the appropriate key usage period and the recommendations shall be acted upon.

3.6. Certificate Renewal

1. The renewal request shall identify the certificate to be renewed.
2. The issuing CA and/or the RA shall ensure that the renewal request is securely submitted and is authenticated as coming from an authorised entity.
3. The issuing CA shall issue a new certificate using the subject's previously certified public key **only if** its cryptographic security is still sufficient for the new certificate's intended lifetime and the requesting subscriber is authorized to request the certificate. In particular, the issuing CA shall not issue a new certificate if:
   a) indications exist that the subject's private key has been compromised;
   b) the previous certificate of the subscriber has been revoked;
   c) the subscriber is still suspended.
4. The issuing CA and/or the RA shall process the certificate renewal data to verify the identity of the requesting entity and identify the certificate to be renewed.
5. The issuing CA shall verify the existence and validity of the certificate to be renewed. No renewal shall be permitted unless the existing certificate status is live (i.e. not revoked or suspended).
6. The issuing CA or the RA shall verify that the request, including the extension of the validity period, meets the requirements defined in the CP.
7. The RA shall secure the part of the certificate renewal process, for which it (the RA) assumes responsibility, in accordance with the CP.
8. The issuing CA shall ensure that renewal actions are recorded in an audit log.
9. The issuing CA shall check the certificate renewal request for errors or omissions. This function can be delegated explicitly to the RA.

10. The issuing CA or RA should notify subjects or, where applicable, subscribers prior to the expiration of their certificate of the need for renewal in accordance with the CP. The notifications from the issuing CA or RA should inform that requests for renewal, rekeying or update of a certificate shall be submitted in due time by the subject. The issuing CA should generate new certificates within the time frame communicated in the notifications to the subject.
11. The issuing CA should issue a signed notification indicating the certificate renewal has been successful.
12. The issuing CA shall make the new certificate available to the end entity in accordance with the CP.
13. The issuing CA shall define terms and conditions in which cases renewal may be allowed
14. The issuing CA shall check duly if the renewal of a certificate is appropriate. Requests to reuse an existing key shall take into account potential weaknesses in the key over the certificate lifetime. Also, it may be necessary to re-check claimed attributes.

3.7. Certificate Revocation & Suspension

1. The issuing CA shall provide a means to facilitate the secure and authenticated revocation of one or more certificates of one or more subjects without undue delay.
2. The issuing CA shall ensure that the revocation request is securely submitted and is authenticated as coming from an authorized entity.
3. The issuing CA shall update the certificate revocation list (CRL), online certificate status protocol (OCSP) responder, or other certificate status mechanisms in the time frames specified within this CP and in accordance with the format defined in ISO/IEC 9594-8 (2022).
4. The issuing CA shall record all certificate revocation requests and their outcome in an audit log.
5. The issuing CA or RA can provide an authenticated acknowledgement (signature or similar) of the revocation to the entity who perpetrated the revocation request.
6. Even if certificate renewal is supported, a revoked certificate shall never be reinstated.
7. The issuing CA should ensure that the subject or the subscriber are notified in the event of a certificate revocation.
8. The system hosting the revocation information shall be protected against system failure and attacks. The Issuing CA shall analyse the risk of a system failure and attacks against the system, taking the assumed traffic into account.
9. The issuing CA shall ensure that the revocation information is secured against unauthorized modification.
10. The issuing CA shall maintain controls to revoke certificates and publish appropriate information about the revoked certificates.
11. In case a legitimate revocation request is received, the issuing CA or a corresponding component service shall update the revocation status information within the time frame specified in the CP or CPS.
12. The issuing CA shall define and implement a process for processing suspension requests in accordance with the CPS. Such a process shall be available to ensure the secure and authenticated suspension of the following:
    a) one or more certificates of one or more subjects;
    b) the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates;
    c) all certificates issued by a CA, regardless of the public/private key pair used.
13. The issuing CA shall ensure that the suspension request is securely submitted and is authenticated as coming from an authorized entity.
14. The issuing CA or RA shall notify the subject and, where applicable, the subscriber in the event of a certificate suspension.
15. Certificate suspension requests shall be processed and validated in accordance with the requirements of the CP.

16. The issuing CA shall update the certificate revocation list (CRL) and other certificate status mechanisms upon certificate suspension. Changes in certificate status shall be completed in a time frame determined by the CP.
17. Certificates shall be suspended only for the allowable length of time in accordance with the CP.
18. Once a certificate suspension (hold) has been issued, the suspension shall be handled in one of the following three ways:
    a) an entry for the suspended certificate remains on the CRL with no further action;
    b) the CRL entry for the suspended certificate is replaced by a revocation entry for the same certificate;
    c) the suspended certificate is unsuspended, and the entry removed from the CRL.
19. A certificate suspension (hold) entry shall remain on the CRL until the expiration of the underlying certificate or the expiration of the suspension, whichever is first. The CP can specify the maximum number of occasions when the certificate status can be suspended and the maximum periodicity for this status.
20. The issuing CA shall update the certificate revocation list (CRL) and other certificate status mechanisms upon the lifting of a certificate suspension in accordance with The issuing CA's CP.
21. The issuing CA shall verify or requires that the RA verify the identity and authority of the entity requesting that the suspension of a certificate be lifted.
22. Certificate suspensions and the lifting of certificate suspensions shall be recorded in an audit log.
23. A certificate should be suspended only if it is likely that private key or other information in the certificate has not been compromised.
24. In case a legitimate suspension request is received, the issuing CA or a corresponding component service shall update the suspension status information within the time frame specified in the CP or CPS.
25. The issuing CA shall ensure that the suspension status information is secured against unauthorized modification.
26. The system hosting the suspension status information shall be protected against system failure and attacks. The issuing CA shall analyse the risk of a system failure and attacks against the system, taking the assumed traffic into account.

4. Other Certificate Policy

4.1. Storage

Certificate and key pairs generated to be stored, managed and backed up using different storage method,

- For low assurance level, for example, a generic purpose certificate, the application could utilize a low-cost, software-based systems, such as commercial browsers.
- For critical applications and servers, a dedicated hardware security module (HSM) or trusted platform module (TPM), which is compliant to appropriate FIPS standard, may be required. Certificate security controls adopt Telstra Cryptography Standard and ISO27099:2022 controls. For technical details, please refer to the corresponding CPS.

5. Appendix

A. Telstra Enterprise Policy & Standard

Document	Version /Date	Status
Telstra Physical Security Standard	V8.0 | Feb.2020	Current
Telstra Cryptography Standard	V7.1 | Feb 2024	Current
Telstra Access Control Standard	V8.1 | Aug 2024	Current
Telstra Data Protection Standard	V4.0 | Feb 2024	Current

B. Industrial & Regulatory Body References

Document	Version /Date	Status
Certificate Policy/Certification Practices Statement for Private PKI Services	V3.14 | Jul 2024	Current
NIST Special Publication 800-152	Oct 2015	Current
NIST Special Publication (SP) 800-57	V7.1 | Feb 2024	Current
NIST Special Publication 800-57 Part 1	Rev 5 | May 2020	Current
NIST Special Publication 800-57 Part 2 Rev1	Rev 1 | May 2019	Current
PCI DSS	Jun 2024	

Note for non-Telstra readers: The contents of this publication are subject to change without notice. All efforts have been made to ensure the accuracy of this publication. Notwithstanding, Telstra Corporation Limited does not assume responsibility for any errors nor for any consequences arising from any errors in this publication.