Controlling Document

Telstra PKI Service
Internal Certificate Policy (MDM)

Published By: Telstra Corporation Ltd

Published Date: Jul 2024

Author:
Telstra PKI Team

Telstra Corporation Limited
ABN 33 051 775 556

Telstra Corporation Limited Certificate Practices Statement

Trademark Notices

REVISION HISTORY

Version	Date	Revision Detail	Author	Status
1.0	July 2024	Review & update	Victor Lew	Current

Table of Contents

1. Purpose

This document provides high level certificate policy requirements for Telstra Intune MDM Certificate Authority (Intune CA) to ensure Telstra PKI provides **Confidentiality**, **Integrity**, **Authenticity** and **Non-repudiation** digital certificate and other relevant PKI services.
This certificate policy document shall be interpreted in accordance with Telstra Cryptography Standard, Telstra Root CA Certification Practice Statement (CPS) and other relevant Telstra PKI documentation.

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 CAs. All capitalized terms in this CP are defined in Telstra Root CA CPS Glossary Section and the provisions for interpretation and construction, severance, waiver and governing law contained in Telstra PKI CPS.

This document does not aim to provide legal advice or recommendations. Telstra MAY publish additional Certificate Policies or Certification Practice Statements, as necessary, to describe other products or service offerings. The Telstra Corporation Limited RCA CPS is published at: http://telstra-pki.pki.telstra.com.au/cps/

2. Scope

This CP intends to cover for Intune Certificate Authority as a Registration Authority for Telstra Root CA.

3. Document Identification

This CP references the Telstra Root Certification Authority Certification Practice Statement (Root CA CPS). The commencement date of this CP is: 28th July 2024
The OID for the Telstra Root CA Certificate Practices Statement (Telstra Root CA CPS) is OID = 11.3.6.1.4.1.1088.4.27.5.2.1

4. Microsoft Intune Certificate Policy

Microsoft Intune uses certificates to authenticate the users' device (in Telstra PKI context, certificates are issued to Telstra MDM devices) to applications and corporate resource across Telstra Network (VPN, WiFi). User use certificates to authenticate these connections. Certificates can also be used for signing and encrypting of email however, this use case is out of scope for current Telstra PKI infrastructure.

Typical use scenarios for certificates include:

- Network authentication (for example, 802.1x) with device or user certs
- Authenticating with VPN servers using device or user certs

4.1. Intune CA (Telstra Issuing CA) High Level Requirements

Below are high level Certificate requirements in accordance with Telstra Cryptography Standard, Telstra Root CA CPS & Technical Detail:

- Intune CA certificate requests shall be accurate, authenticated and approved in accordance with the applicable CPs or CPS.

- Intune CA certificate replacement (renewal and rekey) requests shall be accurate, authorized, and complete in accordance with the applicable CPs or CPS.
- New, renewed, and rekeyed Intune CA certificates shall be generated and issued in accordance with the applicable CPs or CPS.
- Upon issuance, complete and accurate Intune CA certificates shall be made available to relevant entities (subscribers and relying parties) in accordance with the applicable CP(s) or CPS.
- Intune CA certificates shall be revoked based on authorized and validated certificate revocation requests.
- Timely, complete, and accurate certificate status information (including CRLs and other certificate status mechanisms) shall be made available to any entity in accordance with the applicable CP(s) or CPS.

4.2. Certificate Management Process

Telstra Root CA Certificate Management Process within the Telstra PKI includes below major lifecycle stages:

1. Issuance
   a. Enrolment (registration/application)
   b. Signing request
2. Deployment (*key pair generation*)
3. Renewal
4. Revocation

4.3. Certificate Registration and Issuance

Below are high level policies in accordance with Telstra Cryptography Standard, Telstra Root CA CPS & Technical Detail:

- The Intune CA (act as a RA for Telstra Root CA) shall verify or require the credentials presented by a subject as evidence of identity or authority to perform a specific role in accordance with the certificate policy.
- Intune CA shall verify the accuracy of the information included in the requesting entity's certificate request in accordance with the CP.
- The Intune CA shall check the certificate request for errors or omissions in accordance with the CP.
- For end entity certificates, the Intune CA shall ensure that the signing request is securely submitted and is authenticated as coming from an authorized entity.
- Encryption and access controls shall be used to protect the confidentiality and integrity of registration data in transit and in storage.

- At the point of registration (before certificate issuance) the Intune CA shall inform the subject or, where applicable, the subscriber of the terms and conditions regarding use of the certificate.
- Identification and authentication of a subject shall precede any other processes (e.g. certificate issuance) in connection with the subject in question as required by CP.
- A record of registration and related administrative data presented by a subject as evidence of identity shall be kept by the Intune CA.

- The Intune CA shall require that an entity requesting a certificate shall prepare and submit the appropriate certificate request data (registration request) to Intune CA as specified in the CP.
- There shall be evidence of the subjects' agreement to the terms and conditions.
- The Intune CA shall record the success or failure of the registration event in an audit log.
- The Intune CA shall store the certificate enrolment data in a database which is protected against unauthorized access, alteration, and deletion.
- The Intune CA shall ensure that the 'Identification and registration' process is secure. In particular every transfer of registration and identification inside or outside the Intune CA or RA shall be protected against eavesdropping and manipulation.

4.4. Certificate Deployment (Acceptance)

Below are high level policies in accordance with Telstra Cryptography Standard, Telstra Root CA CPS & Technical Detail:

- The Intune CA shall make the certificates issued by Intune CA 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. CD-ROM or hardware token).
- Only authorized CA personnel shall administer The Intune CA's repository or alternative distribution mechanism.
- The performance of The Intune CA's repository or alternative distribution mechanism shall be monitored and managed.
- 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 The Intune CA are made available, The Intune CA shall not issue a certificate for a subject unless that subject's consent for such distribution is obtained.

4.5. Key Pair and Certificate Usage

Below are high level policies in accordance with Telstra Cryptography Standard, Telstra Root CA CPS & Technical Detail.

4.6. Certificate Renewal

Below are high level policies in accordance with Telstra Cryptography Standard, Telstra Root CA CPS & Technical Detail:

- The request shall identify the certificate to be renewed.
- The Intune CA shall ensure that the renewal request is securely submitted and is authenticated as coming from an authorized entity.
- The Intune 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 Intune 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.

- The Intune CA or the RA shall process the certificate renewal data to verify the identity of the requesting entity and identify the certificate to be renewed.
- The Intune 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).
- The Intune CA or the RA shall verify that the request, including the extension of the validity period, meets the requirements defined in the CP.
- The RA shall secure the part of the certificate renewal process, for which it (the RA) assumes responsibility, in accordance with the CP.
- The Intune CA shall ensure that renewal actions are recorded in an audit log.
- The Intune CA shall check the certificate renewal request for errors or omissions. This function can be delegated explicitly to the RA.
- The Intune 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 Intune 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 Intune CA should generate new certificates within the time frame communicated in the notifications to the subject.
- The Intune CA should issue a signed notification indicating the certificate renewal has been
  successful.
- The Intune CA shall make the new certificate available to the end entity in accordance with the CP.
- The Intune CA shall define Terms and Conditions in which cases renewal may be allowed
- The Intune 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.

4.7. Certificate Re-Key

Below are high level policies in accordance with Telstra Cryptography Standard, Telstra Root CA CPS & Technical Detail:

- The Intune CA shall ensure that the rekey request is securely submitted and is authenticated as coming from an authorized entity.
- The Intune CA shall ensure rekey actions are recorded in an audit log.
- The Intune CA or the RA shall check the certificate rekey request for errors or omissions.
- The Intune CA or RA should notify subscribers prior to the expiration of their certificate of the need to rekey.

Prior to the rekeying of existing certificates, The Intune CA or RA shall verify the following:

a) the signature on the certificate rekey data submission;
b) the existence and validity supporting the rekey request;
c) that the request meets the requirements defined in the CP.;
d) the certificate is not revoked, and its subject is not suspended;
e) the new certificate validity period is not extended beyond the expected end of life of the cryptographic algorithm or the key length of the associated key pair;
f) the relevant attributes of the certificate still match the current registration data of the certificate subject.

- Where a new certificate is required by the subscriber, following revocation, the entity shall be required to apply for a new certificate in accordance with the CP.
- Where a new certificate is required by the subscriber following expiration of the entity's certificate, the certificate can be automatically generated, or the entity shall be required to request a new certificate in accordance with the CP.

- The Intune CA shall define Terms and Conditions in which cases rekeying may be allowed.

4.8. Certificate Revocation & Suspension

Below are high level policies in accordance with Telstra Cryptography Standard, Telstra Root CA CPS & Technical Detail:

- The Intune 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.
- The Intune CA shall ensure that the revocation request is securely submitted and is authenticated as coming from an authorized entity.
- The Intune 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 the CP and in accordance with the format defined in ISO/IEC 9594-8.
- The Intune CA shall record all certificate revocation requests and their outcome in an audit log. See Annex C for further guidance.
- The Intune CA or RA can provide an authenticated acknowledgement (signature or similar) of the revocation to the entity who perpetrated the revocation request.
- Even if certificate renewal is supported, a revoked certificate shall never be reinstated.
- The Intune CA should ensure that the subject or the subscriber are notified in the event of a certificate revocation.
- The system hosting the revocation information shall be protected against system failure and attacks. The Intune CA shall analyse the risk of a system failure and attacks against the system, taking the assumed traffic into account.
- The Intune CA shall ensure that the revocation information is secured against unauthorized modification.
- The Intune CA shall maintain controls to revoke certificates and publish appropriate information about the revoked certificates.

- In case a legitimate revocation request is received, The Intune CA or a corresponding component service shall update the revocation status information within the time frame specified in the CP or CPS.
- The Intune 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.
- The Intune CA shall ensure that the suspension request is securely submitted and is authenticated as coming from an authorized entity.
- The Intune CA or RA shall notify the subject and, where applicable, the subscriber in the event of a certificate suspension.

- Certificate suspension requests shall be processed and validated in accordance with the requirements of the CP.
- The Intune 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.

- Certificates shall be suspended only for the allowable length of time in accordance with the CP.
- 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.
- 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.
- The Intune CA shall update the certificate revocation list (CRL) and other certificate status mechanisms upon the lifting of a certificate suspension in accordance with The Intune CA's CP.
- The Intune 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.
- Certificate suspensions and the lifting of certificate suspensions shall be recorded in an audit log. See Annex C for further guidance.
- A certificate should be suspended only if it is likely that private key or other information in the certificate has not been compromised.
- In case a legitimate suspension request is received, The Intune CA or a corresponding component service shall update the suspension status information within the time frame specified in the CP or CPS.
- The Intune CA shall ensure that the suspension status information is secured against unauthorized modification.

- The system hosting the suspension status information shall be protected against system failure and attacks. The Intune CA shall analyse the risk of a system failure and attacks against the system, taking the assumed traffic into account.

5. Other Certificate Policy

5.1. Storage

Certificate and key pairs to use HSM, where is applicable.

5.2. Certificate Security controls

Certificate security controls adopt Telstra Cryptography Standard and ISO27099:2022 controls

5.3. Intune Trust Chain Description

Please refer to Telstra Root CA Technical Detail - Intune for further details.

6. APPENDIX

A. Telstra Internal Policy

- Telstra Access Control Standard
- Telstra Cryptography Standard

B. Intune Reference

Intune supported Certificate type

(Applies to: Android, Android Enterprise, Android (AOSP), iOS/iPadOS, macOS, Windows 8.1, and Windows 10/11)

Select a type depending on how you'll use the certificate profile:

- **User**: *User* certificates can contain both user and device attributes in the subject and SAN of the certificate.
- **Device**: *Device* certificates can only contain device attributes in the subject and SAN of the certificate.

  Use **Device** for scenarios such as user-less devices, like kiosks, or for Windows devices. On Windows devices, the certificate is placed in the Local Computer certificate store.

Key terms:

- Fully managed cloud PKI service (MS)
- Use the Cloud PKI (PKI as Service) to reduce ADCS workload

MS Cloud PKI & Intune Feature

Feature	Overview
Create multiple CAs in an Intune tenant	Create two-tier PKI hierarchy with root and issuing CA in the cloud.
Bring your own CA (BYOCA)	Anchor an Intune Issuing CA to a private CA through Active Directory Certificate Services or a non-Microsoft certificate service. If you have an existing PKI infrastructure, you can maintain the same root CA and create an issuing CA that chains to your external root. This option includes support for external private CA N+ tier hierarchies.
Signing and Encryption algorithms	Intune supports RSA, key sizes 2048, 3072, and 4096.
Hash algorithms	Intune supports SHA-256, SHA-384, and SHA-512.
HSM keys (signing and encryption)	Keys are provisioned using Azure Managed Hardware Security Module (Azure Managed HSM). CAs created with a licensed Intune Suite or Cloud PKI Standalone Add-on automatically use HSM signing and encryption keys. No Azure subscription is required for Azure HSM.
Software Keys (signing and encryption)	CAs created during a trial period of Intune Suite or Cloud PKI standalone Add-on use software-backed signing and encryption keys using System.Security.Cryptography.RSA.
Certificate registration authority	Providing a Cloud Certificate Registration Authority supporting Simple Certificate Enrollment Protocol (SCEP) for each Cloud PKI Issuing CA.

Certificate Revocation List (CRL) distribution points	Intune hosts the CRL distribution point (CDP) for each CA. The CRL validity period is seven days. Publishing and refresh happens every 3.5 days. The CRL is updated with every certificate revocation.
Authority Information Access (AIA) end points	Intune hosts the AIA endpoint for each Issuing CA. The AIA endpoint can be used by relying parties to retrieve parent certificates.
End-entity certificate issuance for users and devices	Also referred to as leaf certificate issuance. Support is for the SCEP (PKCS#7) protocol and certification format, and Intune-MDM enrolled devices supporting the SCEP profile.
Certificate life-cycle management	Issue, renew, and revoke end-entity certificates.
Reporting dashboard	Monitor active, expired, and revoked certificates from a dedicated dashboard in the Intune admin center. View reports for issued leaf certificates and other certificates, and revoke leaf certificates. Reports are updated every 24 hours.
Auditing	Audit admin activity such as create, revoke, and search actions in the Intune admin center.
Role-based access control (RBAC) permissions	Create custom roles with Microsoft Cloud PKI permissions. The available permissions enable you to read CAs, disable and reenable CAs, revoke issued leaf certificates, and create certificate authorities.
Scope tags	Add scope tags to any CA you create in the admin center. Scope tags can be added, deleted, and edited.

C. Intune Certificate Templates & SCEP

Source: https://directaccess.richardhicks.com/2024/03/25/microsoft-intune-cloud-pki-and-certificate-templates/

After deploying Intune Cloud PKI root and issuing CAs, you may wonder where to find the associated certificate templates. If you are familiar with traditional on-premises Active Directory Certificate Services (AD CS) implementations, this is how you define the purpose, key policy, security parameters, and lifetime of the certificate issued using that template. However, Intune Cloud PKI does not use certificate templates in the traditional way many administrators are familiar with.

Note: Microsoft may introduce support for certificate templates for Intune Cloud PKI in the future. However, it is not supported at the time of this writing.

SCEP Profile

Administrators define certificate policies and security parameters using Intune's SCEP device configuration profile instead of certificate templates. In essence, the SCEP profile functions as the certificate template. With the Intune device configuration profile, administrators can define the following settings.

Certificate Type

The certificate type can be either a user or a device. Intune Cloud PKI can issue certificates for either or both, as required.

Subject Name (User)

The subject name is unimportant for user authentication certificates because the User Principal Name (UPN) defined in the Subject Alternative Name field is used to authenticate the user. In this field, the administrator can use whatever they like. However, it's common to use the username here. Avoid using the email attribute here because there's no guarantee that every user will have this defined on the Active Directory (AD) user object.

Subject Name (Device)

Administrators should supply the device's fully qualified domain name (FQDN) for device authentication certificates in the subject name field. For hybrid Entra joined devices, administrators can use the {{FullyQualifiedDomainName}} variable. For native Entra-joined devices, you can use {{DeviceName}} and append your DNS suffix, for example, {{DeviceName}}.corp.example.net.

Note: Intune supports numerous variables to populate fields for certificates. You can find a list of supported variables in the following locations.

- User Certificate Variables;
- Device Certificate Variables

Subject Alternative Name (User)

The Subject Alternative Name (SAN) field for user authentication certificates should be populated with the User Principal Name (UPN) value. Ensure this value is appropriately configured internally and supports sign-in to AD.

Subject Alternative Name (Device)

The SAN field for device authentication certificates should be populated with the device's FQDN. Follow the guidance for device subject names covered previously.

Certificate Validity Period

This field allows the administrator to define the certificate's validity period. The best practice is to limit the lifetime to no more than one year. A shorter lifetime is recommended for certificates not backed by a Trusted Platform Module (TPM).

Key Storage Provider

This value is critical to ensuring integrity for issued user and device authentication certificates. The best practice is to select **Enroll to Trusted Platform Module (TPM) KSP, otherwise fail**. However, if you must issue certificates to endpoints without a TPM (e.g., legacy devices, virtual machines, etc.), consider a separate profile with a shorter certificate lifetime to limit exposure.

Key Usage

Digital signature and Key encipherment are required for user and device authentication certificates.

Key Size

The 2048-bit key size is the minimum recommended value for certificates with RSA keys. Using 4096-bit is not recommended for end-entity certificates and can potentially cause conflicts in some cases**. Intune Cloud PKI does not support the 1024-bit key size.**

Hash Algorithm

SHA-2 is the best practice for the hash algorithm. SHA-1 has been deprecated and should not be used.

Root Certificate

Select the Cloud PKI root CA certificate.

Extended Key Usage

The minimum requirement for user and device authentication certificates is Client Authentication (1.3.6.1.5.5.7.3.2).

Renewal Threshold

This value specifies at what point the certificate can be renewed. 20% is commonly used for certificates with a one-year lifetime.

SCEP Server URLs

This value can be found on the configuration properties page of your Cloud PKI issuing CA. The URI will include a variable in the URL. The variable is there by design. Copy and paste this URL exactly as displayed in the SCEP URL field.

D. Policy & Standard

Document	Version /Date	Status
Telstra Physical Security Standard	V8.0 | Feb.2020	Current

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.