Apple Inc.

Apple Issuing Authority Root Certification Practice Statement

Version 1.0

Effective Date: April 21, 2025

Table of Contents

1. INTRODUCTION

1.1. OVERVIEW

This Certification Practice Statement ("CPS") describes the practices employed by Apple Inc. ("Apple") acting as a Root CA and Subordinate CA that issues Derived ID Credential Document Signing Certificates ("Apple CA").

Root Certificates issued by the Apple CA, and described herein, are intended to be trusted by the United States Transportation Security Administration (TSA) and other Relying Parties that display or use Certificates and incorporate Root Certificates, including Apple. As such, the Apple CA inherits the responsibilities outlined in the current version of the TSA Digital ID Requirements, Version 2.0 ("DI Requirements").

The Apple CA issues Root Certificates and Subordinate CA Certificates ("Sub-CA Certificate") for Apple.

The Apple CA also issues Derived ID Credential Document Signing Certificates ("Subscriber Certificates") and manages related services to digitally sign Derived Identity Credential documents stored on the holder's mobile device for Apple.

This CPS provides the practices for issuance of all Apple Issuing Authority Certificates, including Root Certificates, Sub-CA Certificates and Subscriber Certificates. These practices are designed to conform to the requirements in the current version of the DI Requirements. This CPS further defines the practices relating to Certificate lifecycle services, such as issuance, management, and revocation, as well as details relating to other business, legal, and technical matters.

This CPS is structured according to RFC 3647, and includes at least every section and subsection defined in RFC 3647.

1.2. DOCUMENT NAME AND IDENTIFICATION

This is the Apple Issuing Authority Root CPS, defining the practices required of the Certification Authority for issuance of Derived ID Credential Document Signing Certificates.

1.2.1. Revisions

This CPS is reviewed and updated as REQUIRED by updates to the DI Requirements. The following revisions have been made to the original document:

Date	Changes	Version
April 21, 2025	Initial release.	1.0

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

A Certification Authority ("CA") is an organization that is authorized to issue, manage, and revoke Certificates. The Apple CA, acting as the Issuing Authority (IA) Certificate Authority (IACA), is the Root CA and Subordinate CA for Apple.

1.3.2. Registration Authorities

A Registration Authority ("RA") performs identification and authentication checks for end-user Certificate Applicants. The Apple CA acts as a Registration Authority. This function is not delegated to a third party.

1.3.3. Subscribers

A Subscriber is a Legal Entity that has been issued a Certificate signed by an Apple CA. Apple, acting as the Issuing Authority (IA), is the Subscriber of Derived ID Credential Document Signing Certificates.

1.3.4. Relying Parties

A Relying Party is any natural person or Legal Entity that relies on a Valid Certificate issued by the Apple CA.

1.3.5. Other Participants

1.3.5.1. Apple CA Policy Authority

The Apple Policy Authority (APA) is a multi-disciplinary group from within Apple and its subsidiaries, responsible for interpretation of requirements, maintenance, and approval of this CPS.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate Certificate Uses

The Apple CA issues and administers X.509 Certificates for signing Derived Identity Credentials.

1.4.2. Prohibited Certificate Uses

The Apple CA does not allow its Subscribers' Certificates to sign other Certificates, nor does it allow its Sub-CA Private Keys to sign other Sub-CA Certificates.

Certificates issued by the Apple CA SHALL not be used for any purpose that is not identified in Section 1.4.1 as a permitted use.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

This CPS is administered by the APA.

1.5.2. Contact Person

The contact information for this CPS is:

Apple CA Policy Authority
One Apple Park Way
Cupertino, CA 95014

(408) 996-1010
policy_authority@apple.com

1.5.3. Person Determining CPS Suitability for the Policy

The APA determines the suitability and applicability of this CPS.

1.5.4. CPS Approval Procedures

This CPS and all its amendments are subject to approval by the APA. The CPS MAY change at any time without prior notice. Amendments to this CPS will be evidenced by a new version number and date and recorded in the revision table in Section 1.2.1, except where the amendments are purely clerical.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

See Appendix A.1.

1.6.2. Acronyms

See Appendix A.2.

1.6.3. References

This CPS adopts the DI Requirements — Digital ID Risk Controls table References column. References not included in the above document will be listed below.

1.6.4. Conventions

The key words “MUST”, “MUST NOT”, "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in the policies, guidelines, and requirements mentioned in Section 1.1. have been interpreted in accordance with RFC 2119.

By convention, this CPS omits time and timezones when listing effective requirements such as dates. Except when explicitly specified, the associated time with a date is 00:00:00 UTC.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

The Apple CA repository is composed of multiple documents, made available in publicly accessible areas:

- Status information for Subscriber Certificates,
- Root Certificates and Sub-CA Certificates,
- The current version of this CPS and the Relying Party Agreement, and
- Results of the annual WebTrust audit.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

The latest versions of this CPS, Relying Party Agreement, Root Certificates and Sub-CA Certificates are published at https://www.apple.com/certificateauthority/apki202505 and are readily accessible on a 24x7 basis.

Certificate status information MAY also be checked via the Certificate Revocation List ("CRL"), which is published by the Apple CA on a periodic basis. Refer to the CRL Distribution Point extension in the Certificates for the status information method used as described in Section 7.1.2.

2.3. TIME OR FREQUENCY OF PUBLICATION

Updates to this CPS are published as necessary.

Certificate status information for Subscriber Certificates is published as specified in Section 4.9.7 for CRLs.

Root Certificates and Sub-CA Certificates are published as soon as possible after issuance.

2.4. ACCESS CONTROLS ON REPOSITORIES

Read-only access to information in public repositories is provided without restriction.

The Apple CA has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

Certificates contain a Subject defined in Section 7.1.

3.1.2. Need for Names To Be Meaningful

Certificates are issued with a non-null subject DN that conforms with ITU X.500.

3.1.3. Anonymity Or Pseudonymity Of Subscribers

Generally, the Apple CA does not issue Certificates with pseudonyms.

3.1.4. Rules of Interpreting Various Name Forms

Distinguished names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.5. Uniqueness of Names

See Section 7.1

3.1.6. Recognition, Authentication, and Role of Trademarks

Apple, iOS, and macOS are trademarks of Apple Inc. in the United States and other countries.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Method To Prove Possession of Private Key

The Certificate Applicant MUST demonstrate that it rightfully holds the Private Key corresponding to the Public Key listed in the Certificate by submitting a PKCS#10 Certificate Signing Request ("CSR").

3.2.2. Authentication of Organization Identity

The Apple CA verifies the identify and address of the organization and that the address is the Applicant's address of existence or operation using documentation provided by, or through communication with a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition.

3.2.3. Authentication of Individual Identity

The Apple CA does not issue Subscriber Certificates to an Applicant who is a natural person.

3.2.4. Non-Verified Subscriber Information

The Apple CA does not include non-verified Subscriber information in Certificates.

3.2.5. Validation of Authority

Apple CA verifies authority by confirming the presence of the Certificate Requester in a pre-vetted list of authorized users.

3.2.6. Criteria for Interoperation

No stipulation.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-Key

See Section 4.7.

3.3.2. Identification and Authentication for Re-Key After Revocation

See Section 4.7.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

Identification and authentication for revocation requests is performed in compliance with Section 4.9 of this document.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

Root Certificate and Sub-CA Certificate

Only individuals in Trusted Roles working for the Apple CA MAY submit Certificate Applications for Root Certificates and Sub-CA Certificates.

Subscriber Certificates

A Certificate Requester representing the Applicant MAY submit Certificate Applications.

4.1.2. Enrollment Process and Responsibilities

The Apple CA has an enrollment process for Subscriber Certificates which MAY include the following:

- A Terms of Use,
- Information about the Applicant including, but not limited to, organization name, contacts, and authorizing individuals,
- Certificate Signing Request (CSR)
- Appropriate approvals by the Applicant.

Prior to issuing a Certificate, the Apple CA MAY collect evidence from sources other than the Applicant to confirm information to be included in the Certificate.

The Apple CA MAY leverage the verification information for an Applicant such as Legal existence, Address of Place of Business, Verified Method of Communication and Operational Existence. The use of this information is limited to the maximum age specified in Section 4.2.1.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

As part of this validation process, Apple CA authenticates Subject information using the procedures described in Section 3.2.2. Certificate Applications are not approved unless Apple CA has obtained all necessary information as specified in Section 4.1.2.

4.2.2. Approval or Rejection of Certificate Applications

The Apple CA rejects Certificate Applications that cannot be verified based on the practices outlined in Section 4.2.1.

4.2.3. Time to Process Certificate Applications

No stipulation.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions During Certificate Issuance

A Certificate is created and issued following approval of the Certificate Application.

Root Certificates and Sub-CA Certificates

The Apple CA generates CA Certificates during a scripted ceremony, conducted by trusted personnel observing separation of duties and two-person controls consistent with Section 5.2. Ceremonies for Root Certificates are witnessed by a qualified person.

Subscriber Certificates

The Apple CA's enrollment system will use the information provided as part of the verification practices in Section 3.2.2, data in the online submission, and configuration constraints. Among other things, the system will:

- use the Public Key in the CSR,
- populate verified data in the Subject DN

4.3.2. Notification To Subscriber by the CA of Issuance of Certificate

Upon issuance of a Certificate, the Apple CA MAY notify the Subscriber by sending an email to the mailbox address associated with the Certificate Application.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2. Publication of the Certificate by the CA

See Section 2.1.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No stipulation for Subscriber Certificates.

For Root and Sub-CA Certificates see Section 2.1.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Certificate use MUST be consistent with the permitted uses described in Section 1.4.1.

Prior to using a Certificate, Subscribers represent that they will comply with the obligations outlined in Section 9.6.3. by accepting the Terms of Use.

4.5.2. Relying Party Public Key and Certificate Usage

See Section 9.6.4.

4.6. CERTIFICATE RENEWAL

Certificate renewal is the issuance of a new Certificate to the Subscriber with the same Public Key and verified information (e.g. identity, domains, email address) in the Certificate. A renewed Certificate has a new serial number and an expiration date ending after the expiration date of the Certificate being renewed.

4.6.1. Circumstance for Certificate Renewal

No stipulation.

4.6.2. Who May Request Renewal

No stipulation.

4.6.3. Processing Certificate Renewal Requests

No stipulation.

4.6.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6. Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7. CERTIFICATE RE-KEY

Certificate re-key is the issuance of a new Certificate to the Subscriber with a new Public Key and same verified information (e.g. identity) in the Certificate. A re-keyed Certificate has a new serial number and same expiration date in the Certificate being re-keyed.

4.7.1. Circumstance for Certificate Re-Key

No stipulation.

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.

4.7.1. Notification of Certificate Issuance by the CA to Other Entities.

No stipulation.

4.8. CERTIFICATE MODIFICATION

Certificate modification means the issuance of a new Certificate to the Subscriber with the same Public Key but different verified information (e.g. identity) in the Certificate. A modified Certificate has a new serial number and same or other expiration date ending after the expiration date of the Certificate being modified.

4.8.1. Circumstance for Certificate Modification

No stipulation.

4.8.2. Who May Request Certificate Modification

No stipulation.

4.8.3. Processing Certificate Modification Requests

No stipulation.

4.8.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6. Publication of the Modified Certificate by the CA

No stipulation.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

The Apple CA provides revocation information for all Certificates issued by its Root Certificates and Sub-CA Certificates.

4.9.1. Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

A Subscriber MAY request revocation of its Certificate at any time for any reason.

Subscriber Certificates

The Apple CA MAY revoke a Subscriber Certificates after confirming one or more of the following occurred:

1. The Subscriber requests in writing, without specifying a reason, that the Apple CA revoke the Certificate,
2. The Subscriber notifies the Apple CA that the original Certificate Application was not authorized and does not retroactively grant authorization,
3. The Apple CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise,
4. The Apple CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate,
5. The Apple CA obtains reasonable evidence that the Certificate has been misused or used for a purpose outside of that indicated in the Certificate,
6. The Apple CA confirms that a Subscriber has violated one or more of its material obligations under any relevant agreement,
7. The Apple CA confirms a material change in the information contained in the Certificate,
8. The Apple CA confirms that the Certificate was not issued in accordance with this CPS,
9. The Apple CA confirms that any of the information appearing in the Certificate is inaccurate,
10. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of this CPS,

11. The Apple CA confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed,

12. The Private Key used by the Apple CA to issue the Certificate is suspected to have been compromised.

4.9.1.2. Reasons for Revoking a Sub-CA Certificate

The Apple CA MUST revoke a Sub-CA Certificate after confirming one of the following occurred:

1. The APA requests revocation in writing,
2. The Apple CA becomes aware than the original request for the Sub-CA Certificate was not authorized and does not retroactively grant authorization,
3. The Private Key corresponding to the Public Key in the Sub-CA Certificate suffered a Key Compromise or no longer complies with the requirements of this CPS Sections 6.1.5 and 6.1.6,
4. The Apple CA obtains evidence that the Sub-CA Certificate was misused,
5. The Apple CA is made aware that the Sub-CA Certificate was not issued in accordance with this CPS,
6. The Apple CA determines that any of the information appearing in the Sub-CA Certificate is inaccurate or misleading,
7. The Apple CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate.

4.9.2. Who Can Request Revocation

For Subscriber Certificates, the Subscriber who requested the original Certificate MAY request the revocation of the Certificate.

The Apple CA reserves the right to revoke any Certificates, without notice, for any reason.

4.9.3. Procedure for Revocation Request

The Apple CA provides an online revocation process available 24x7 to Subscribers. The Subscriber will be required to authenticate to the enrollment system with their Identification Credential. After authentication, the requestor requests revocation of their Certificate and then the Certificate will be automatically revoked. After the Certificate is revoked, a revocation notification is sent to the Subscriber.

If a revocation is required for a Sub-CA Certificate, the Compliance team will engage the APA for revocation approval and a ceremony will be promptly scheduled.

4.9.4. Revocation Request Grace Period

No stipulation.

4.9.5. Time Within Which CA Must Process the Revocation Request

A revocation request submitted to the online enrollment system is processed immediately.

4.9.6. Revocation Checking Requirement for Relying Parties

Relying Parties are solely responsible for performing revocation checking on all Certificates in the chain before deciding whether or not to rely on the information in a Certificate. The Apple CA provides revocation status via mechanisms that are embedded in the Certificate (e.g., CRL Distribution Point).

4.9.7. CRL Issuance Frequency

For the status of Sub-CA Certificates, the Apple CA issues a new CRL at least once every twelve (12) months. CRLs are issued with a nextUpdate time at most twelve (12) months from the thisUpdate time. When a Sub-CA Certificate is revoked, a new CRL will be generated within forty-eight (48) hours.

Within forty-eight (48) hours of issuing its first Certificate from a new sub-CA, the Apple CA generates and publishes a complete CRL. Afterwards, CRLs are continuously issued until all Sub-CAs associated to the Public Key used to sign the CRL are expired or revoked.

For the status of Subscriber Certificates, the Apple CA issues a new CRL (i.e., thisUpdate) at least once every forty-eight (48) hours. CRLs are issued with a nextUpdate time no longer than 7 days from the thisUpdate time.

The Apple CA makes CRLs publicly-accessible via an HTTP URL, which is disclosed in the Certificate itself as shown in profiles in Section 7.1.

4.9.8. Maximum Latency for CRLs

No stipulation.

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 Related to Key Compromise

See Section 4.9.1

4.9.13. Circumstances for Suspension

The Apple CA does not support Certificate suspension.

4.9.14. Who Can Request Suspension

No stipulation.

4.9.15. Procedure for Suspension Request

No stipulation.

4.9.16. Limits on Suspension Period

No stipulation.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

The Apple CA offers Certificate status information using CRLs and Certificate status services are available via the CRL Distribution Point noted in the Certificates.

Revocation entries on a CRL are available until after the expiration date of the revoked Certificate.

4.10.2. Service Availability

No stipulation.

4.10.3. Operational Features

No stipulation.

4.11. END OF SUBSCRIPTION

A Subscriber MAY end subscription for a Certificate by allowing the Certificate to expire, or by revoking the Certificate prior to expiration.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

The Apple CA implements management, operational and physical controls as specified in the DI Requirements.

5.1. PHYSICAL SECURITY CONTROLS

5.1.1. Site Location and Construction

Equipment supporting CA operations resides within a physically secured location in geographically separated Apple owned or controlled facilities.

5.1.2. Physical Access

Physical protection is achieved through the creation of clearly defined security perimeters with appropriate physical barriers to entry around the business premises, data center, and CA operations.

Data center site physical security mechanisms include facility design and construction, perimeter security (e.g., heavy duty fences, gates, and barriers), and logical and personnel controls (e.g., access management, badging, and multi-factor authentication).

Within the data center, additional security controls are placed on the High Security Environments ("HSE") housing CA operations. Separate logical and physical security mechanisms protect the HSEs, situated in either cages or secured rooms, and include access management controls, such as two-person access and multi-factor authentication.

By default, access to the CA operations room or cage is disabled for all personnel, with access provisioning granted on an as-needed basis for specific time intervals. Access to safes protecting assets requires two-person control.

Apple's global security team is responsible for physical access to Apple data centers and HSEs, including access management systems, access records, monitoring and alerting systems, and security personnel to provide a continuous presence at each data center facility.

5.1.3. Power and Air Conditioning

Equipment is protected to reduce risks from power and air conditioning disruption or failure. Power is maintained in emergency situations by uninterrupted power supplies and generators. Redundant power supplies are tested on a regular basis.

5.1.4. Water Exposures

Equipment is protected to reduce risks from water exposure by means of temperature and humidity monitoring.

5.1.5. Fire Prevention and Protection

The data centers are protected with fire suppression systems, alarms, and monitors.

5.1.6. Media Storage

Media is maintained securely within the CA facilities and is subject to the same degree of protection as the CA hardware. Backups are stored at secondary data center locations, as per Section 5.1.8.

5.1.7. Waste Disposal

Media used to collect sensitive information is destroyed or zeroized prior to disposal.

Cryptographic devices are physically destroyed or zeroized in accordance with manufacturer's guidance prior to disposal.

5.1.8. Off-Site Backup

Backups are taken at regular intervals and stored at alternate locations as described in Section 5.4.5. For purposes of backup and recovery, offline Root and Sub-CA Private Keys, which are stored in encrypted form, are transported to alternate secure storage under dual control. The backups exist in multiple copies in different geographic locations.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

Individuals in Trusted Roles have access to or control over cryptographic operations, including access to restricted operations within the Apple CA. Individuals in Trusted Roles MUST be Apple employees whose identity has been confirmed through background checking procedures as defined in Section 5.3 and who have accepted the responsibilities of a Trusted Role. Functions performed by persons in Trusted Roles are distributed in such a manner that prevents one person from subverting the security and trustworthiness of CA operations.

Procedural controls for individuals in Trusted Roles include:

1. Administrative access to Certificate Systems is granted only to individuals in Trusted Roles.
2. Administrative access to Certificate Systems is removed whenever a person's authorization is changed or revoked.
3. Appointments to Trusted Roles and assignment of responsibilities are made per documented processes.
4. Separation of duties are implemented for task and responsibilities individuals in Trusted Roles.
5. Access to High Security Environments and other Secure Zones is only granted to individuals in Trusted Roles.
6. Administrative tasks are defined for each type of Trusted Role; individuals are restricted from actions beyond the scope of their assigned role.

7. Certificate Systems are configured to observe the principle of least privilege for each Trusted Role type.
8. Each individual in a Trusted Role authenticates to Certificate Systems using a unique credential. Group accounts are not used.
9. Workstations and Certificate Systems are configured to log out or lock when no longer used.
10. Remote administration of Certificate Systems is restricted and protected by means of encrypted channels, multi-factor authentication, and secure network.

The responsibilities for each of the Trusted Roles include administration and operation tasks as described in the sections below.

5.2.1.1. CA Administrator

The CA Administrator is responsible for installation, configuration, and maintenance of the CA software, configuring Certificate Profiles, and generating and backing up Root and Sub-CA keys. CA Administrators do not issue Certificates to Subscribers.

5.2.1.2. RA Officer

The RA Officer, also known as a Validation Specialist, is responsible for verifying the identity of Applicant / Subscribers and accuracy of information included in Certificates, approving and executing the issuance of Certificates, and requesting the revocation of Certificates.

5.2.1.3. Audit Administrator

The Audit Administrator is responsible for reviewing, maintaining, and archiving audit artifacts and performing or overseeing internal compliance audits to ensure that the CA and other systems are operating in accordance with this CPS.

5.2.1.4. Operator

Operators, such as system administrators and CA operators, are responsible for keeping systems updated with software patches, hardware upgrades, and other maintenance needed for system stability and recoverability.

5.2.1.5. RA Administrator

RA Administrators install, configure and manage the RA software, including Sub-CAs and Certificate Profiles.

5.2.2. Number of Persons Required per Task

Root and Sub-CA Private Keys are backed up, stored, and recovered by individuals in Trusted Roles under multi-person control in a physically secured environment.

Subscriber Private Keys are managed under multi-person control as described in Section 6.1.1.3 and Section 6.2.2.

Contractors serving in Trusted Roles will perform their functions under the supervision of a second Trusted Role individual who is an Apple employee.

5.2.3. Identification and Authentication for Each Role

Individuals in Trusted Roles identify and authenticate themselves using multi-factor authentication, including a certificate-based credential, before being allowed access to the systems necessary to perform their Trusted Roles.

The Apple CA temporarily locks access to secure CA processes if more than 5 consecutive login attempts fail.

5.2.4. Roles Requiring Separation of Duties

To accomplish separation of duties, Apple CA specifically designates individuals to specific Trusted Roles as described in Section 5.2.1 above.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

Individuals in Trusted Roles are Apple personnel who have successfully completed a background check consistent with federal, state, and local regulations and have demonstrated the trustworthiness, skills and experience to accept Trusted Role responsibilities. Personnel in Trusted Roles undergo training prior to performing any duties as part of that role.

5.3.2. Background Check Procedures

Apple implements several processes at both time of hire and throughout an employee's tenure to assess and validate an individual's identity and trustworthiness.

5.3.2.1. Identity verification

Apple employees complete identity verification at time of hire. U.S. based Apple employees successfully complete the verification by means of government-issued photo identification compliant with the requirements of the U.S. Department of Homeland Security Form I-9 Employment Eligibility Verification.

5.3.2.1. Trustworthiness assessment

Apple employees are REQUIRED to successfully complete a background check at time of hire. Background checks can include both criminal and non-criminal services (i.e. education verification and previous employment verification) consistent with federal, state, and local regulations.

Every Apple employee's performance is reviewed on a yearly basis to ensure they are meeting Apple's high standards.

5.3.3. Training Requirements and Procedures

Individuals in Trusted Roles performing Certificate System duties receive skills-training prior to commencing their job role.

5.3.4. Retraining Frequency and Requirements

Apple employees complete training at time of hire and on an ongoing basis. Annual training includes but is not limited to: Worldwide Business Conduct, Privacy, and Compliance and Security training, with required modules determined by role and access level.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of policies and procedures. Disciplinary actions MAY include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7. Independent Contractor Requirements

Contractors are allowed to serve in certain Trusted Roles. Contractors are subject to training practices described in Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

5.3.8. Documentation Supplied to Personnel

Policies and procedures are posted in an internal site that is made available to individuals in Trusted Roles.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

Apple CA configures its Certificate Systems, Certificate Management Systems, and Root CA Systems to record essential security events. When specific events cannot be logged automatically, manual procedures are put in place to record the event.

The Apple CA records the following events:

1. CA certificate and key lifecycle events, including:
    i. Key generation, backup, storage, recovery, archival, and destruction,
    ii. Request of Certificate issuance, renewal, modification, re-key, and revocation,
    iii. Approval and rejection of certificate requests above in Section 5.4.1 (1)(ii),
    iv. Cryptographic device lifecycle management events,
    v. Generation of Certificate Revocation Lists, and
    vi. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:

i. Request of Certificate issuance, renewal, modification, re-key, and revocation,
ii. All verification activities stipulated this CPS,
iii. Approval and rejection of certificate requests above in Section 5.4.1 (2)(i),
iv. Issuance of Certificates, and
v. Generation of Certificate Revocation Lists.

3. Security events, including:
   i. Successful and unsuccessful PKI system access attempts,
   ii. PKI and security system actions performed,
   iii. Security profile changes,
   iv. Installation, update and removal of software on a Certificate System,
   v. System crashes, hardware failures, and other anomalies,
   vi. Firewall and router activities, and
   vii. Entries to and exits from the CA facility.

For each event, the Apple CA records the date and time, type of event, and user or system that caused the event or initiated the action.

5.4.2. Frequency of Processing and Archiving Audit Logs

Apple CA reviews system logs at least monthly to detect anomalies or irregularities. Automated tools are used to alert for specific conditions. Reviewed activities are tracked and documented, and are made available to external auditors upon request.

5.4.3. Retention Period for Audit Logs

Certificate System logs are retained for minimum of 36 months.

Audit logs are retained for a minimum of two (2) years after the following:

1. For CA certificate and key lifecycle management event records (specified in Section 5.4.1(1)), after the later occurrence of:
   i. the destruction of the CA Private Key, or
   ii. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key,
2. For Subscriber Certificate lifecycle management event records (specified in Section 5.4.1(2)), after the expiration of the Subscriber Certificate,
3. For security event records (as specified in Section 5.4.1(3)) after the event occurred.

Apple CA makes these audit logs available to its external auditor upon request.

5.4.4. Protection of Audit Log

Online audit logs are maintained securely within the CA facilities and are subject to the same degree of protection as the CA hardware. Archived audit logs are maintained in a secondary storage location as per Section 5.4.5. CA system configurations and operational procedures ensure that only authorized personnel MAY read or archive audit logs, and that audit logs are protected from unauthorized modification or deletion.

5.4.5. Audit Log Backup Procedures

Systems hosting audit data are backed up daily, The data is replicated to a secondary site, which is in a geographically separated Apple facility. Audit logs are archived monthly and retained for the duration of the retention period described in Section 5.4.3.

5.4.6. Audit Collection System (Internal Vs. External)

Audit logs are collected using enterprise-grade storage management systems, stored only within Apple data centers, as defined in Section 5.4.5.

5.4.7. Notification To Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

Apple CA performs an annual risk assessment to:

- Identify threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes,
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes, and
- Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.5. RECORDS ARCHIVAL

5.5.1. Types of Records Archived

The Apple CA archives records of the events listed in Section 5.4.1.

5.5.2. Retention Period for Archive

Records listed in Section 5.5.1 above are retained for at least two (2) years after any Certificate ceases to be valid or as long as they are required to be retained per Section 5.4.3, whichever is longer. Apple CA also retains archived documentation

relating to the verification, issuance, and revocation of certificate requests and Certificates after the later occurrence of:

- such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
- the expiration of all the Subscriber Certificates relying upon such records and documentation.

5.5.3. Protection of Archive

Archive records are maintained in a manner to prevent unauthorized modification, substitution, or destruction.

The systems hosting the archived data therein are subject to authentication and authorization mechanisms, redundancy, backup storage in secondary sites, equipment updates and media refreshes.

Apple ensures that the archived records are retained in the software systems until no longer needed, or migrated to a replacement system in the event that the record retention requirement is longer than the lifespan of the software system.

5.5.4. Archive Backup Procedures

The Apple CA archives are backed up to storage in a different, geographically separated, Apple owned or controlled facility or service.

5.5.5. Requirements for Time-Stamping of Records

The systems hosting the archived data automatically timestamp archive records as they are created. System time is synchronized using the Network Time Protocol (NTP). Cryptographic time-stamping of archive records is not performed.

5.5.6. Archive Collection System (Internal or External)

Apple CA collects archive information internally.

5.5.7. Procedures to Obtain and Verify Archive Information

Apple restricts access to archive data to authorized trusted personnel and Apple staff only, in accordance with internal procedures and security policies. Apple does not release any archived information except as allowed by law as specified in Section 9.

5.6. KEY CHANGEOVER

Towards the end of each Root CA or Sub-CA lifetime, a new CA Key Pair is generated following the procedures in Section 6.1.1.1.

The old Root CA Private Key will no longer be used to sign new Sub-CA Certificates. All subsequently issued Sub-CA Certificates issued from the new Root CA are signed with the new Private Key

The old Sub-CA Private Key will no longer be used to sign new Subscriber Certificates, but will be used to sign CRLs. All subsequently issued Subscriber Certificates and CRLs issued from the new Sub-CA are signed with the new Private Key.

Towards the end of the Subscriber Certificate lifetime, a new Subscriber Key Pair is generated following the procedures in Section 6.1.1.3.

The Apple CA will continue to protect its old Private Keys, and makes the old Root, Sub-CA, and Subscriber Certificates available to verify signatures at least until all of the Certificates signed with the respective Private Key have expired.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

The Apple CA maintains an Incident Response Plan and a Disaster Recovery Plan as specified in Digital ID Risk Controls Sections 1.9.6 and 1.9.10 of the DI Requirements.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

In the event of a disaster in which computing resources, software, and/or data is corrupted, appropriate escalation, incident investigation, and response will be initiated. The Apple CA will halt the issuance or validation of Certificates if compromise of those systems, or data, MAY cause the generation of Certificates or status responses that do not comply with this CPS.

In the event of a disruption, when restoring operations, the Apple CA will give priority to reestablishing the generation of Certificate status information.

5.7.3. Entity Private Key Compromise Procedures

In the event of compromise, suspected compromise, or loss of a Root or Sub-CA Private Key, appropriate escalation, incident investigation, and response will be initiated. This response will include filing an incident report as described in Digital ID Risk Controls Sections 1.9.6 and 1.9.10 of the DI Requirements.

If the investigation confirms the need for revocation of a Sub-CA Certificate, the Apple CA will revoke the compromised Certificate. Subsequently, a new CA Key Pair will be created, and a new Sub-CA Certificate created. The Apple CA will also revoke, and if necessary reissue, all impacted Subscriber Certificates.

If a Root Certificate is compromised, the Apple CA will work with IA to address the retirement of the Certificate in an orderly manner. Actions prior to retirement MAY include the revocation of all Sub-CA and Subscriber Certificates and subsequent re-issuance.

5.7.4. Business Continuity Capabilities After a Disaster

The Disaster Recovery Plan noted in Section 5.7.1 relies on preparation before a disaster event as well as actions triggered by the disaster event.

Prior to a disaster event, systems are REQUIRED to be architected with multiple redundant layers and are allocated in multiple geographically diverse locations to provide continuous operation. Risk vectors are re-evaluated continuously and the plan is strengthened based on findings.

When a disaster impacts one of the redundant layers, the other layers will continue operations without, or with minimal, interruption.

5.8. CA OR RA TERMINATION

Apple CA will execute the termination plan that addresses the following:

- Provision of notice to parties affected by the termination,
- The revocation of Certificates issued by the Apple CA,
- The preservation of the Apple CA's archives and records.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

6.1.1.1. CA Key Pair Generation

The Apple CA generates CA Key Pairs used in Root and Sub-CA Certificates during a scripted ceremony, conducted by trusted personnel, observing separation of duties and two-person controls consistent with Section 5.2, witnessed by external qualified auditors. A report is produced by the auditors opining on the ceremony.

Ceremonies are conducted in secure facilities described in Section 5.1. CA Key Pairs are generated using FIPS-validated Cryptographic Modules complying with Section 6.2.1. The ceremony produces evidence available to auditors to verify that appropriate controls were met.

6.1.1.2. RA Key Pair Generation

No stipulation.

6.1.1.3. Subscriber Key Pair Generation

The Apple CA does not generate Key Pairs for Subscriber Certificates. These Key Pairs are generated by the Subscriber. The Apple CA requires that Subscriber Key Pairs be generated with a documented and auditable multi-party Key Ceremony. The Subscriber, at a minimum, SHALL perform the following:

- Prepare and follow a Key Generation Script;
- Generate the Subscriber Certificate Key Pairs in a physically secured environment as described in Section 5.1;
- Generate the Subscriber Certificate Key Pairs using personnel in Trusted Roles under the principles of two-person control and split knowledge.

Before including a Subscriber's key in a Certificate, the Key is verified to meet the minimum sizes specified in Section 6.1.5. Keys that do not meet those specifications result in their associated Certificate Application being rejected.

6.1.2. Private Key Delivery to Subscriber

The Apple CA does not generate and deliver key pairs for Subscriber Certificates.

6.1.3. Public Key Delivery to Certificate Issuer

Public Keys for Subscriber Certificates are submitted using a PKCS#10 CSR over a TLS connection.

6.1.4. CA Public Key Delivery to Relying Parties

Root and Sub-CA Certificates are hosted in the online Repository indicated in Section 2.1.

6.1.5. Key Sizes

6.1.5.1. Root Certificates

See Section 7.1.

6.1.5.2. Sub-CA Certificates

See Section 7.1.

6.1.5.3. Subscriber Certificates

See Section 7.1.

6.1.6. Public Key Parameters Generation and Quality Checking

No Stipulation.

6.1.7. Key Usage Purposes (as per X.509 v3. Key Usage Field)

See Section 7.1.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

Root Private Keys are generated and stored in Cryptographic Modules that are certified as FIPS 140-3 level 3. Sub-CA Private Keys are generated and stored in Cryptographic Modules that are certified as FIPS 140-2 level 3.

Apple CA requires that Subscriber Keys be generated and stored using NIST FIPS 140-2 Level 3 certified HSMs.

6.2.2. Private Key (n out of m) Multi-Person Control

The Apple CA generates Root CA and Sub-CA Key Pairs, including backups, and activates Private Keys for signature operations in a physically secure environment, under multi-person control by individuals in Trusted Roles.

6.2.3. Private Key Escrow

Root and Sub-CA Private Keys are backed up but not escrowed.

6.2.4. Private Key Backup

The Apple CA backs up its Root CA and Sub-CA Private Keys in a physically secure environment, under multi-person control by individuals in Trusted Roles, storing at least one backup at a secure secondary location. All copies of its Root and Sub-CA Private Keys are protected in the same manner as the original.

6.2.5. Private Key Archival

The Apple CA does not archive Private Keys used in Root Certificates or Sub-CA Certificates.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

Transfer of the Root and Sub-CA Private Key into or from a Cryptographic Module, performed only for key backup procedures, is done in accordance with the manufacturers' guidelines, under multi-person control by individuals in Trusted Roles. The Apple CA never allows the Private Keys to exist in plaintext outside of these Cryptographic Modules at any point in time.

6.2.7. Private Key Storage on Cryptographic Module

Root and Sub-CA Private Keys, including backups, are stored in Cryptographic Modules that meet the specifications in Section 6.2.1.

Apple CA requires that the Subscriber Certificate Keys, including backups, are to be stored in Cryptographic Modules that meet the specifications in Section 6.2.1.

6.2.8. Method of Activating Private Key

Activation of Root and Sub-CA Private Keys is done in accordance with the guidelines provided by the manufacturer of the Cryptographic Module, under multi-person control, performed by individuals in Trusted Roles. Activation data will be protected from disclosure or communication to any external party.

Apple CA requires that activation of Subscriber Certificate Keys be done under multi-person control, performed by individuals in Trusted Roles.

6.2.9. Method of Deactivating Private Key

Sub-CA Private Keys are deactivated upon executing a deactivation command. Root Private Keys are deactivated upon system power off. The Apple CA prevents unauthorized access to any activated Cryptographic Modules.

6.2.10. Method of Destroying Private Key

Root and Sub-CA Private Keys on Cryptographic Modules will be destroyed by individuals in Trusted Roles in accordance with instructions and documentation provided by the manufacturer, when no longer needed.

6.2.11. Cryptographic Module Rating

See specification in Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

No Stipulation.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The operational period for Key Pairs is the same as the Validity Period for associated Certificates. See Section 7.1.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

The Apple CA follows the manufacturer specifications for the activation data required for Root and Sub-CA Private Keys. As specified in Section 6.2.2, to activate a Cryptographic Module, M of N secrets are REQUIRED. Those secrets are generated when the Cryptographic Module is initialized and they are stored on separate secure tokens.

6.4.2. Activation Data Protection

The Apple CA protects from disclosure the data used to unlock Private Keys using a combination of cryptographic and physical access control mechanisms. Secure tokens with activation data are kept under multi-person control, as specified in Section 5.1.2, and require a PIN of minimum eight (8) digits to unlock for use.

The Apple CA locks access to secure CA processes if a certain number of failed password attempts occur as specified in Section 5.2.3.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

The Apple CA configures systems to meet the following security technical requirements, at a minimum:

- User identities are authenticated before access is permitted to systems or applications,
- User privileges are managed to limit users to their assigned roles,
- Audit records are generated and archived for applicable transactions,
- Domain integrity boundaries are enforced for security critical processes, and
- Recovery is supported for key or system failures.

The Apple CA enforces multi-factor authentication on any account capable of directly causing Certificate issuance.

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

The Apple CA acquires CA and OCSP Responder software from a reputable third-party. The vendor has an established software development life-cycle management process.

The Apple CA develops some software modules in-house, also following an established software development life-cycle management process.

For Apple CA operations, this software is installed on dedicated hardware.

Purchases of hardware and software assets are conducted using established procurement processes and delivered using tracked and verifiable mechanisms in order to reduce the likelihood of tampering

The Apple CA uses a formal configuration management methodology for installation and ongoing maintenance of any CA system. Any modifications or upgrades to the system are documented and controlled.

6.6.2. Security Management Controls

The Apple CA system configurations are periodically reviewed to identify any unauthorized changes.

The Apple CA maintains change control mechanisms to document, control, monitor, and maintain the installation and configuration of the CA systems, including any modifications or upgrades. When loading software onto a CA system, the Apple CA verifies that the software is the correct version and is supplied by the vendor free of any modifications.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

Network security measures are in place to protect against denial of service and intrusion attacks, including denying all but the necessary services to support the CA systems, network segmentation, access limited to CA personnel, and regular review of network, firewall, ACL, and load balancer configurations. Initial configurations are reviewed to verify that all versions are correct and are set as supplied by the vendor free of any modifications.

6.8. TIME-STAMPING

Apple CA systems are continuously synchronized using the Network Time Protocol ("NTP") by means of NTP pools dedicated to each Apple data center. NTP services on CA systems are monitored to ensure the NTP service is running and to detect if the system clock is out of synchronization with UTC.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

The Apple CA issues Certificates with the content and extensions shown below. All extensions are set in accordance with RFC 5280. Extensions are not marked critical unless specifically described as critical.

Root CA Certificate

Field or extension	Value
Serial Number	A non-sequential number containing at least 64 bits of output from a CSPRNG
Issuer Distinguished Name	C=US, Organization=Apple Inc., CN=Apple Issuing Authority ECC Root CA - G[generation] Generation: A numeric value that starts with one (1) and increases by one (1) when a new Certificate, that supersedes an existing one, is issued by the same Root Certificate.
Subject Distinguished Name	Same as Issuer DN
Subject Public Key Info	P-384 key: secp384r1
Signature Algorithm	ecdsa-with-SHA384
Validity Period	Up to 7300 days
Basic Constraints	Critical. CA = True pathLenConstraint is not present
Subject Key ID	The 160-bit SHA-1 hash of the value of the BIT STRING subject Public Key
Key Usage	Critical. Key certificate sign, CRL Sign
Issuer Alternate Name	https://www.apple.com/certificateauthority/apki202505

Subordinate CA Certificate

Field or extension	Value
Serial Number	A non-sequential number containing at least 64 bits of output from a CSPRNG.
Issuer Distinguished Name	Derived from the Issuing CA

Field or extension	Value
Subject Distinguished Name	C=US, Organization=Apple Inc., CN=Apple Issuing Authority ECC CA [number] - G[generation] Number: A numeric value that uniquely distinguishes the CA Certificate from others within the same type/algorithm pair. For Sub-CA Certificates, the number is unique across the entire Root Certificate naming space. Generation: A numeric value that starts with one (1) and increases by one (1) when a new Certificate, that supersedes an existing one, is issued by the same Root Certificate.
Subject Public Key Info	P-384 key: secp384r1
Signature Algorithm	ecdsa-with-SHA384
Validity Period	Up to 5475 days
Basic Constraints	Critical. CA = True pathLenConstraint = 0
Authority Key ID	Identical to the subject Key Identifier field of the Issuing CA
Subject Key ID	The 160-bit SHA-1 hash of the value of the BIT STRING subject Public Key
Key Usage	Critical. Key certificate sign, CRL Sign
Extended Key Usage	1.0.18013.5.1.2 (mdlDS) 1.0.23220.4.1.2 (mdocDS)*
CRL Distribution Point	Contains a CRL URL which varies based on Issuing CA
Subject Alternate Name	https://www.apple.com/certificateauthority/apki202505
Certificate Policies	1.2.840.113635.100.5.22.1.1 (Apple Certificate Policy)

Subscriber Certificate

Field or extension	Value
Serial Number	A non-sequential number containing at least 64 bits of output from a CSPRNG.
Issuer Distinguished Name	Derived from the Issuing CA
Subject Distinguished Name	C=US, Organization=Apple Inc., CN=Apple Derived ID Credential Document Signing
Validity Period	Up to 450 days
Subject Public Key Info	P-256 key: secp256r1
Signature Algorithm	ecdsa-with-SHA256
Basic Constraints	CA = False

Field or extension	Value
Authority Key ID	Identical to the subject Key Identifier field of the Issuing CA
Subject Key ID	The 160-bit SHA-1 hash of the value of the BIT STRING subject Public Key
Key Usage	Critical. Digital Signature
Extended Key Usage	Critical. 1.0.18013.5.1.2 (mdlDS) 1.0.23220.4.1.2 (mdocDS)*
Authority Information Access	Contains a CA Issuers URL
CRL Distribution Point	Contains a CRL URL which varies based on Issuing CA
Issuer Alternate Name	https://www.apple.com/certificateauthority/apki202505
Certificate Policies	1.2.840.113635.100.5.22.1.1 (Apple Certificate Policy) CPS Policy Qualifier: https://www.apple.com/certificateauthority/apki202505 User Notice Qualifier: Reliance on this certificate by any party assumes acceptance of the Relying Party Agreement found at https://www.apple.com/certificateauthority/apki202505

Note: The OID 1.0.23220.4.1.2 (mdocDS) is documented in FINAL DRAFT of Technical Specification ISO/IEC DTS 23220-4.

7.1.1. Version Numbers

Certificates issued under this CPS are X.509 version 3.

7.1.2. Certificate Content and Extensions

See Section 7.1.

7.1.3. Algorithm Object Identifiers

7.1.3.1. SubjectPublicKeyInfo

See Section 7.1.

7.1.3.2. Signature AlgorithmIdentifier

See Section 7.1.

7.1.4. Name Forms

7.1.4.1. Subject Attribute Encoding

Apple CA includes the Subject attributes in the tables below in Root CA, Subordinate CA and Subscriber Certificates. These attributes are included in a Certificate only after validation is completed in accordance with Section 3.2.

Attribute	Encoding	Max Length	Presence
countryName	PrintableString	2	Yes
organizationName	UTF8String	64	Yes
commonName	UTF8String	64	Yes

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

See Section 7.1.

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

See Section 7.1.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

For the status of Subordinate CA Certificates:

Field or extension	Value
Version	v2
Signature Algorithm	ecdsa-with-SHA384
Issuer Name	Derived from the Issuing CA
ThisUpdate	The date and time with the CRL validity begins
NextUpdate	Up to ThisUpdate + twelve (12) months
RevokedCertificates	Contains serial number of the revoked certificate and the revocation date. CRL entry extensions SHALL not be used.
Authority Key ID	Identical to the subject Key Identifier field of the Issuing CA
CRLnumber	Sequential CRL number, increased monotonically as each new CRL is issued

For the status of Subscriber Certificates:

Field or extension	Value
Version	v2
Signature Algorithm	ecdsa-with-SHA256
Issuer Name	Derived from the Issuing CA
ThisUpdate	The date and time with the CRL validity begins
NextUpdate	Up to ThisUpdate + 7 days
RevokedCertificates	Contains serial number of the revoked certificate and the revocation date. CRL entry extensions SHALL not be used.
Authority Key ID	Identical to the subject Key Identifier field of the Issuing CA
CRLnumber	Sequential CRL number, increased monotonically as each new CRL is issued

7.2.1. Version Number

See Section 7.1.

7.2.2. CRL and CRL Entry Extensions

See Section 7.1.

7.3. OCSP PROFILE

No stipulation.

7.3.1. Version Number

No stipulation.

7.3.2. OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The audit against TSA Digital ID Requirements is performed at least every three years. The WebTrust audit is performed annually.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The TSA Digital ID Requirements audit MUST be conducted by an independent third-party assessor chosen from the FedRamp approved third-party assessor list (https://www.fedramp.gov/assessors/).

The auditors performing the annual WebTrust audit are from an independent audit firm that is approved to audit according to CPA Canada WebTrust for Certification Authorities Principles and Criteria.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

An independent external audit firm will be retained.

8.4. TOPICS COVERED BY ASSESSMENT

The audit will meet the requirements of the current version of the TSA Digital ID Requirements.

For the WebTrust audit, the auditor will assess controls to the current version of CPA Canada Trust Service Principles and Criteria for Certification Authorities.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The Apple CA Policy Authority will determine the significance of identified deficiencies arising from external audits or internal self-assessments, and will prescribe remediation requirements. The Apple CA Policy Authority will be responsible for seeing that remediation efforts are completed in a timely manner.

8.6. COMMUNICATION OF RESULTS

Copies of the latest WebTrust audit reports can be found in the Repository as specified in Section 2.1.

8.7. SELF-AUDITS

No stipulation.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

The Apple CA does not charge fees for any services related to Certificate issuance or Certificate validation described in this CPS.

9.2. FINANCIAL RESPONSIBILITY

To the extent permitted by applicable law Apple disclaims any warranties, including any warranty of merchantability or fitness for a particular purpose. All Relying Parties must bear the risk of reliance on any Certificates issued by the Apple CA.

9.2.1. Insurance Coverage

Apple maintains general liability insurance coverage.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

The following information is considered Apple confidential and protected against disclosure and may not be disclosed:

- Private Keys and data used to access the CA system,
- Business and security plans including but not limited to business continuity, incident response, contingency, and disaster recovery plans,
- Security mechanisms used to protect the confidentiality, integrity, or availability of information,
- Information held by the Apple CA as personal or non-public information in accordance with Section 9.4, and
- Transaction records, audit logs, archival records, financial audit records, and external or internal audit trail records and any audit reports.

9.3.2. Responsibility To Protect Confidential Information

Confidential information will not be released to any third parties unless required by law or requested by a court with jurisdiction over the Apple CA. Apple's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle

confidential information. The confidential information will be kept confidential even after the termination of this CPS.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

The Apple CA follows the Apple privacy policy which is available at https://www.apple.com/legal/privacy.

9.4.2. Information Treated as Private

See Section 9.4.1.

9.4.3. Information Not Deemed Private

Any information publicly available through a Certificate, CRL or their contents is not deemed private.

9.4.4. Responsibility To Protect Private Information

See Section 9.4.1.

9.4.5. Notice and Consent To Use Private Information

See Section 9.4.1.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

See Section 9.4.1.

9.4.7. Other Information Disclosure Circumstances

See Section 9.4.1.

9.5. INTELLECTUAL PROPERTY RIGHTS

Apple and/or its business partners own the intellectual property rights in Apple CA's services, including the Certificates, CRLs, trademarks used in providing the services, the policies and procedures supporting the operations of such services, the CA infrastructure, and this CPS. Apple, iOS, and macOS are trademarks of Apple Inc., in the United States and other countries.

Apple grants permission to reproduce and distribute Certificates on a nonexclusive and royalty-free basis, provided that they are reproduced and distributed in full. Private Keys and Public Keys remain the property of the Subscribers who rightfully hold them. All secret shares (distributed elements) of the Apple Private Keys are the property of Apple.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, Apple does not make any representations regarding its products or services. To the

extent permitted by applicable law Apple disclaims any warranties, including any warranty of merchantability or fitness for a particular purpose.

Subject to the terms and conditions of this CPS and any applicable agreement between the parties, Apple represents that it:

- Complies in all material aspects with this CPS, and all applicable laws and regulations,
- Has verified all Certificates issued by the Apple CA using the processes outlined in this CPS,
- Publishes and updates CRLs on a regular basis (See Section 4.9.7),
- Meets the minimum requirements in the set forth in Section 1.1, and
- Maintains a Repository (See Section 2.1).

9.6.2. RA Representations and Warranties

Subject to the terms and conditions of this CPS and any applicable agreement between the parties, RAs represent that:

- The RA's Certificate issuance and management services conform to this CPS, and
- All Certificates requested by the RA meet the requirements of this CPS.

9.6.3. Subscriber Representations and Warranties

Subscribers are solely responsible for any information provided as part of a Certificate Application and for all transactions that use the Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify the Apple CA if a change occurs that could affect the status of the Certificate, or if they believe that the Certificate information or Private Key have been compromised or are no longer valid or secure.

The Terms of Use includes the following Subscriber requirements and obligations:

- Securely generating its Private Keys and protecting its Private Keys from compromise,
- Providing accurate and complete information when communicating with the Apple CA,
- Confirming the accuracy of the Certificate Data prior to using the Certificate,
- Promptly

- requesting revocation of a Certificate, cease using it and its associated Private Key, and notify the Apple CA if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate, and
- requesting revocation of the Certificate, and ceasing using it, if any information in the Certificate is or becomes incorrect or inaccurate,

- Ensuring that individuals managing Certificates on behalf of an organization have received security training appropriate to the Certificate,
- Using the Certificate only for authorized and legal purposes, consistent with the Certificate purpose, this CPS, and the Terms of Use, and
- Promptly cease using the Certificate and related Private Key after the Certificate's expiration.

The Terms of Use may include additional representations and warranties.

9.6.4. Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a Certificate issued by the Apple CA, it:

- Obtained sufficient knowledge on the use of Certificates and PKI,
- Studied the applicable limitations on the usage of Certificates and agrees to Apple's limitations on liability related to the use of Certificates,
- Has read, understands, and agrees to their Apple Relying Party Agreement and this CPS,
- Verified all Certificates in the certificate chain using the relevant CRL,
- Will not use an expired or revoked Certificate, and
- Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a Certificate after considering:
  - applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction,
  - the intended use of the Certificate as listed in the Certificate or this CPS,
  - the data listed in the Certificate,
  - the economic value of the transaction or communication,

- the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
- the Relying Party's previous course of dealing with the Subscriber,
- the Relying Party's understanding of trade, including experience with computer-based methods of trade, any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction, and
- any reliance on a Certificate is at the party's own risk.

Relying Party Agreements may include additional representations and warranties.

9.6.5. Representations and Warranties of Other Participants

The parties agree that there are no third-party beneficiaries, other than those specifically identified herein under this CPS and any other applicable agreement.

9.7. DISCLAIMERS OF WARRANTIES

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, APPLE DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. APPLE DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. APPLE DOES NOT GUARANTEE THE AVAILABILITY OF ANY PRODUCTS OR SERVICES AND MAY MODIFY OR DISCONTINUE ANY PRODUCT OR SERVICE OFFERING AT ANY TIME.

9.8. LIMITATIONS OF LIABILITY

ANY ENTITY USING AN APPLE CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF APPLE RELATED TO SUCH USE, PROVIDED THAT THE APPLE CA HAS COMPLIED WITH THIS CPS IN PROVIDING THE CERTIFICATE OR SERVICE. APPLE'S LIABILITY FOR CERTIFICATES AND SERVICES THAT DO NOT MATERIALLY COMPLY WITH THIS CPS IS LIMITED AS SET FORTH IN THE APPLE RELYING PARTY AGREEMENT. THEY FURTHER ACKNOWLEDGE THAT THE CERTIFICATES ARE NOT INTENDED OR SUITABLE FOR USE IN SITUATIONS OR ENVIRONMENTS WHERE THE FAILURE OR TIME DELAYS OF, OR ERRORS OR INACCURACIES IN THE CONTENT, DATA OR INFORMATION PROVIDED BY, THE CERTIFICATES AND SERVICES COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE, INCLUDING WITHOUT LIMITATION THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT OR WEAPONS SYSTEMS.

All liability is limited to actual and legally provable damages. Apple is not liable for:

- Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if Apple is aware of the possibility of such damages,
- Liability related to fraud or willful misconduct of the Applicant,
- Liability related to use of a Certificate that exceeds the limitations on use, value, or transactions as stated either in the Certificate, this CPS or any applicable Relying Party agreement,
- Liability related to the security, usability, or integrity of products not supplied by Apple, including the Subscriber's and Relying Party's software or hardware, or
- Liability related to the compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether Apple failed to follow any provision of this CPS, or (v) whether any provision of this CPS was proven ineffective.

The disclaimers and limitations on liabilities in this CPS are fundamental terms to the use of Certificates and services provided by the Apple CA.

To the extent the Apple CA has issued and managed the Certificate(s) at issue in compliance with this CPS, Apple shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). To the extent permitted by applicable law, and Relying Party Agreements shall limit Apple's and the applicable Affiliates' liability. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9. INDEMNITIES

9.9.1. Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify Apple, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Terms of Use, this CPS, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence or intentional acts; (iv) Subscriber's misuse of the Certificate or Private Key; or (v) failure to notify the Apple CA that the Private Key and its accompanying Certificate have been compromised or are no longer valid.

The Terms of Use may include additional indemnity obligations.

9.9.2. Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify Apple, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Relying Party , regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Relying Party's breach of the Relying Party Agreement, this CPS, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Relying Party's negligence or intentional acts; (iv) Relying Party's misuse of the Certificate or Private Key, or (v) failure to notify the Apple CA that the Private Key and its accompanying Certificate have been compromised or are no longer valid.

The applicable Relying Party Agreement may include additional indemnity obligations.

9.10. TERM AND TERMINATION

9.10.1. Term

The CPS and/or Relying Party Agreement, and any amendments thereto, become effective upon publication to the Repository (See Section 2.1). The CPS and relevant agreements will continue until either an updated version is published to the Repository, (see Section 2.1), or they are terminated in accordance with the CPS or the termination provisions of the applicable agreement.

9.10.2. Termination

This CPS is amended from time to time, and shall remain in effect until replaced by a newer version.

9.10.3. Effect of Termination and Survival

Upon termination of this CPS, Terms of Use and/or Relying Party Agreement, Subscribers and Relying Parties are nevertheless bound by their terms for all Certificates issued for the remainder of the validity periods of such Certificates, until replaced by newer versions of those documents.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Apple may provide notice and provide updates to this CPS, Terms of Use and/or Relying Party Agreement by making them available in the Repository, see Section 2.1. Notices and updates to this CPS by Apple are deemed effective upon availability in the Repository.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

This CPS is reviewed as frequently as necessary, but at least once a year. This CPS the Terms of Use, and/or Relying Party Agreement may be amended at any time and will be published in the Repository(See Section 2.1). Updates supersede any designated or conflicting provisions of the referenced version of the CPS. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the Apple CA Policy Authority.

9.12.2.Notification Mechanism and Period

Apple CA may make changes to this CPS without notice.

9.12.3.Circumstances Under Which OID Must Be Changed

The Apple CA Policy Authority is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13. DISPUTE RESOLUTION PROVISIONS

Any litigation or other dispute resolution related to the use of the Certificates in this CPS will take place in the Northern District of California, and Relying Parties consent to the personal jurisdiction of and exclusive venue in the state and federal courts within that District with respect to any such litigation or dispute resolution.

Parties are required to notify the Apple CA and attempt to resolve disputes directly with the Apple CA before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14. GOVERNING LAW

Under this CPS, the rights and obligations of the parties shall be governed by and construed and enforced under the laws of the State of Delaware, without regard to its choice of law principles, except that the arbitration clause below, and any arbitration hereunder, shall be governed by the United States Federal Arbitration Act, Chapters 1 and 2. The Convention on Contracts for the International Sale of Goods shall not apply to this CPS.

9.15. COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to all applicable laws and regulations.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

This CPS, the Terms of Use, and the applicable Relying Party Agreement represent the entire agreement, and contractually obligates each Subscriber, Relying Party and RA to comply with this CPS. The Apple CA also requires each party using its products and services to enter into an agreement that delineates the terms associated with

the product or service. Third parties may not rely on or bring action to enforce such agreement.

9.16.2.Assignment

Entities operating under this CPS may not assign their rights or obligations without the prior written consent of Apple. Any assignment made in violation of this section shall be voided upon Apple's request.

9.16.3.Severability

If a provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable.

9.16.4.Enforcement (Attorneys' Fees and Waiver of Rights)

Apple may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. Apple's failure to enforce a provision of this CPS does not waive Apple's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by Apple.

9.16.5.Force Majeure

Apple is not liable for a delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond Apple's reasonable control. The operation of the Internet is beyond Apple's reasonable control.

9.17. OTHER PROVISIONS

No stipulation.

Appendix A: Definitions and Acronyms

A.1 DEFINITIONS

Table A-1 Definitions

Term	Definition
Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.
CA Key Pair	A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).
Certificate	An electronic document that uses a digital signature to bind a public key and an identity.
Certificate Application	The document, physical or electronic, submitted by an Applicant to Apple CA for the purpose of obtaining a Certificate.
Certificate Data	Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
Certificate Management System	A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Profile	A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7, e.g. a Section in a CA's CPS or a certificate template file used by CA software.
Certificate Requester	A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant that completes and submits an Certificate Application on behalf of the Applicant.
Certificate Revocation List (CRL)	A regularly updated time, stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
Certificate Systems	The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.

Term	Definition
Certification Authority (CA)	An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs. See Section 1.3.1.
Certification Practice Statement (CPS)	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
CSPRNG	A pseudo-random number generator intended for use in a cryptographic system.
Delegated Third Party	A natural person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
Delegated Third Party System	Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by the CA.
Derived Identity Credential	An identity credential issued by Apple that is derived from government-issued passports.
Digital Identity Document	A government-issued identity document that is issued in a machine-processable form, that is digitally signed by the issuer, and that is in purely digital form.
Expiry Date	The , "Not After", date in a Certificate that defines the end of a Certificate's validity period.
High Security Environment	A physical location where a CA's or Delegated Third Party's Private Key or cryptographic hardware is located.
Incident	A CA's failure to comply with any requirement of this CPS - whether it be a misissuance, a procedural or operational issue, or any other variety of non-compliance.
Individual	A Natural Person.
Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Issuing System	A system used to sign certificates or validity status information.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair.
Key Pair	The Private Key and its associated Public Key.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Term	Definition
Multi-Factor Authentication	An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction: something you know (knowledge factor), something you have (possession factor), and something you are (inherence factor). Each factor MUST be independent. Certificate-based authentication can be used as part of Multifactor Authentication only if the private key is stored in a Secure Key Storage Device.
Natural Person	An Individual; a human being as distinguished from a Legal Entity.
Object Identifier (OID)	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Pseudonym	A fictitious identity that a person assumes for a particular purpose. Unlike an anonymous identity, a pseudonym can be linked to the person's real identity.
Public Key	The key of a Key Pair that MAY be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Public Key Infrastructure (PKI)	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 8.2.
Registration Authority (RA)	Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. See Section 1.3.2.
Relying Party	Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate. Section 1.3.4.
Repository	An online database containing publicly, disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Requirements	The collection of Requirements as listed in Section 1.1.

Term	Definition
Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
Root CA Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
Root CA System	A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.
Secure Key Storage Device	A device certified as meeting at least FIPS 140-2 level 2 overall, level 3 physical, or Common Criteria (EAL 4+).
Secure Zone	An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device or mailbox under the control and operation of the Subscriber.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber	A natural person or Legal Entity to whom a Certificate is issued. See Section 1.3.3.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
System	One or more pieces of equipment or software that stores, transforms, or communicates data.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with this CPS when the Applicant/ Subscriber is an Affiliate of the CA or is the CA.
Trusted Role	An employee or contractor of a CA or Delegated Third Party who has authorized access to or control over a Secure Zone or High Security Environment.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialist	Someone who performs the information verification duties specified by these Requirements.
Validity Period	From RFC 5280, "The period of time from notBefore through notAfter, inclusive."
Zone	A subset of Certificate Systems created by the logical or physical partitioning of systems from other Certificate Systems.

A.2 ACRONYMS

Table A-2 Acronyms

Acronym	Term
DN	Distinguished Name
DI	Digital Identification
IA	Issuing Authority
IACA	Issuing Authority Certificate Authority
IDN	Internationalized Domain Name
mDL	Mobile Driver's License
TSA	Transportation Security Administration