Apple Inc.
Certification Practice Statement
Apple IST CAs

Version 1.0
Effective Date: August 25, 2014

1. Introduction

1.1. Overview

This Certification Practice Statement ("CPS") describes the practices employed by the Apple IST Subordinate Certification Authorities ("the Apple IST CAs" or "the Sub-CAs") in issuing and managing digital certificates and related services. It defines policies that the Sub-CAs are required to follow, provides additional information about the practices employed by the Sub-CAs relating to certificate lifecycle services, such as issuance, management, revocation, renewal, and rekeying, as well as details relating to other business, legal, and technical matters specific to the Apple IST CAs, collectively referred to as the Apple IST Public Key Infrastructure ("Apple IST PKI").

1.2. Document naming and identification

This is the Apple IST Certification Practice Statement. The object identifier values corresponding to the Certificate Policy is:

- appleCABFSSLBaselineCertificatePolicy: 1.2.840.113635.100.5.11.4

Subscriber certificates containing this policy identifier fall under the scope of this certificate practice statement.

1.3. PKI participants

1.3.1. Certification authority (CA)

This is an entity that is authorized to issue, manage, revoke, and renew Certificates under the Apple IST CAs.

1.3.2. Registration authority (RA)

The Registration Authority performs identification and authentication checks for end-user certificate applicants. The Subordinate CAs within the scope of this CPS act as the Registration Authority.

1.3.3. Subscriber

This is an entity who has been issued a Certificate signed by an Apple IST Sub-CA. All Subscribers are internal to Apple.

1.3.4. Relying party

This is any entity that receives an X.509 certificate (issued to a subscriber by an Apple IST Sub-CA) and has an interest of some kind in the validity of the certificate.

1.3.5. Other participants

None.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

1.4.1.1. TLS Server and Client Certificates

The Apple IST CAs issue and administer X.509 Certificates with a Server Authentication and/or Client Authentication Extended Key Usage (EKU) used to provide server authentication, data encryption, message integrity, and optional client authentication.

1.4.2. Prohibited certificate uses

The Apple IST CAs do not allow its Certificates to be used to create a Certification Authority or to allow its private key to sign a Certificate issued by another Certification Authority.

Except for internal-use Certificates, the Apple IST Sub-CA Certificates 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

The CA's Certificate Policies are administered by the Apple CA Policy Authority.

1.5.2. Contact person

The contact information for this CPS is:

Apple CA Policy Authority
1 Infinite Loop
Cupertino, CA 95014
(408) 996-1010
policy_authority@apple.com

1.5.3. CPS Approval Procedure

This CPS and all amendments to this CPS is subject to approval by the Apple CA Policy Authority. 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 History, except where the amendments are purely clerical.

1.6. Definitions and acronyms

The following acronyms are used within this document. This table describes the general meaning of these terms as used.

Acronym	Term
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement

CRL	Certificate Revocation List
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
PA	Apple CA Policy Authority
PKI	Public Key Infrastructure
RA	Registration Authority
Root CA	Root Certification Authority
Sub-CA	Subordinate Certification Authority

The following terms are used within this document. This section describes the general meaning of these terms as used.

Term	Definition
Certificate	A document structured as specified in the ASN-1 language and formatted according to the X.509 standard that contains information such as a distinguished name, common or full name, electronic mail address, validity period, and public key.
Certificate Application	The process whereby a subscriber requests a CA to perform a key administration function; or, requests a CA to issue or revoke a certificate. This may also be defined as the document submitted by a subscriber to a CA for the purpose of obtaining a certificate or requesting the CA to perform an administrative function.
Certification Authority	This is an entity that is authorized to issue, manage, revoke, and renew Certificates under the Apple IST CAs.
Certification Authority Management Team (CA Management Team)	The group of people within Apple responsible for defining CA policy and supporting ongoing operations.
Certificate Chain	This is a collection of certificates that are considered as a group to verify the authenticity of a particular certificate. In the usual X.509 certificate model, the certificate to be verified ("leaf") is a certificate issued by a subsidiary CA to a subscriber. The certificate for the subsidiary CA is in turn signed by the root CA certificate. Each issued certificate contains a digital signature signed by its issuer. The digital signature can be verified at the request of a relying party by both the subsidiary and root CA so as to authenticate the source and integrity of the certificates and any objects signed or encrypted using the related public/private keys.
Certificate Policy/Certification Practice Statement	This is a corporate policy that sets forth business practices, system integrity controls, environmental controls, and specific operational practices and procedures associated with the Apple IST CAs.

Term	Definition
Certificate Revocation List	This is a digitally signed list of certificates that are no longer valid because the accompanying private key has been lost, stolen, or compromised, or the CA has revoked the certificate. As an example: A relying party may check to see if a certificate that they receive is listed on a CA's revocation list. If the Certificate is listed, the relying party knows that any signature or source of an encrypted object should not be trusted as of the date the CA added the certificate to the CRL.
Directory	A system operated and administered by a CA that supports the storage and retrieval of X.509 certificates and CRLs managed by the CA. This system may support X.500 Directory Services, or implement similar technology. Whatever service is used, it should support the X.520 naming convention (distinguished names) to uniquely identify every subscriber to whom a certificate is issued by a CA. This may also be referred to as a repository.
Distinguished Name	Within the scope of a CA related to the issuance and management of certificates, this is a value that uniquely identifies each entity or resource to which a certificate is issued.
Hardware Security Module	A self-contained hardware device that provides cryptographic services used to protect an information system. Trust and integrity are derived from the security of the signing and encryption keys stored within. Cryptographic key material is securely stored within a tamper resistant (FIPS 140-2 Level 3 or higher) device.
Online Certificate Status Protocol	This is a protocol that provides the ability to determine the revocation status of a digital certificate without CRLs.
Private Key	The key of a Key Pair kept secret by its holder, used to create Digital Signatures and to decrypt messages or files that were encrypted with the corresponding Public Key.
Public Key	The key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and used by the recipient to validate Digital Signatures created with the corresponding Private Key and to encrypt messages or files to be decrypted with the corresponding Private Key.
Public Key Infrastructure	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based Public Key Cryptography system.
Relying Party	This is any entity that receives an X.509 certificate (issued to a subscriber by an Apple IST Sub-CA) and has an interest of some kind in the validity of the certificate.
Repository	As used, same as Directory.
Root Certification Authority	This is a CA that is at the top of a hierarchical PKI network.

Term	Definition
Subscriber	This is an entity who has been issued a Certificate signed by an Apple IST Sub-CA. All Subscribers are internal to Apple.
Subordinate Certification Authority	This is a CA that is a node of the Root CA within a hierarchical PKI network.

2. Publication and Repository Responsibilities

2.1. Repositories

The Apple IST CAs operate a private repository of issued certificates, which is not publicly accessible.

2.2. Publication of certification information

The latest version of this CPS in published at www.apple.com/certificateauthority.

Certificate status information may be made available through the Online Certificate Status Protocol ("OCSP"). Certificate status information may also be checked via the Certificate Revocation List ("CRL") which is published by Apple on a periodic basis. Refer to the CRL Distribution Point ("CDP") or the Authority Information Access ("AIA") extensions in the Certificates for the status information method used.

2.3. Time or frequency of publication

Updates to this CPS are published to www.apple.com/certificateauthority as necessary. Certificate status information for Subscriber Certificates is published via OCSP at least every four days and via CRL at least every seven days.

2.4. Access controls on repositories

There is no public repository of certificates. Subscribers shall have access to their own Certificates through an internal process.

This CPS is publicly available at www.apple.com/certificateauthority.

Certificate status information is publicly available via CRL or OCSP, which will be provided in the manner described by the CRL Distribution Points, or the Certificate Authority Information Access (AIA) extension present in the leaf Certificates issued by an Apple IST CA.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

Certificates contain a Distinguished Name in the Subject name field and consist of the components noted below:

3.1.1.1. TLS Server and Client Certificates

Field/Attribute	Value
Country (C)	US
State (ST)	California
Organization (O)	Apple Inc.
Common Name	<A Fully –Qualified Domain Name (FQDN) in the list of approved Apple-owned domains>

3.1.2. Need for names to be meaningful

Domain names do not have to be meaningful but must be in the list of approved domains.

3.1.3. Anonymity or pseudonymity of subscribers

Not applicable.

3.1.4. Rules of interpreting various name forms

Not applicable.

3.1.5. Uniqueness of names

Not applicable.

3.1.6. Recognition, authentication, and role of trademarks

Apple, OS X, and iOS 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

All certificates issued from the Apple IST CAs will have an organization identity (O) of Apple Inc.

3.2.3. Authentication of individual identity

The issuance of a Certificate from an Apple IST CA is contingent upon the requesting Subscriber being an Apple staff member. The Subscriber requests a certificate after authentication with the appropriate credentials.

3.2.3.1. TLS Client and Server Authentication

The CA will take reasonable steps to establish that a Certificate request is for an approved Apple-owned domain.

3.2.4. Non-verified subscriber information

Non-verified Subscriber information includes:

- Any value noted as non-verified in the Certificate.

3.2.5. Validation of authority

The CA will take reasonable steps to establish that a Certificate request is from Apple staff. Subscribers must authenticate with the appropriate credentials before a Certificate request can be submitted.

3.2.6. Criteria for interoperation

Not applicable.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

Subscribers may request certificate rekey in case of key compromise or certificate expiration. Certificate rekey requests follow the same process as the initial certificate issuance.

3.3.2. Identification and authentication for re-key after revocation

Subscribers may request certificate rekey in case of key compromise. Certificate rekey requests follow the same process as the initial certificate issuance.

3.3.3. Identification and authentication for revocation requests

The certificate revocation process will commence upon receipt of a valid request to revoke the set of Certificates from the Subscriber. The Subscriber will be required to authenticate. After authentication, the Subscriber will indicate that they wish to revoke their Certificate. Once a certificate has been revoked, its revocation status cannot be modified. An email is sent to the Subscriber to notify that the certificate has been revoked.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who can submit a certificate application

Only valid Apple staff may submit certificate requests.

4.1.2. Enrollment process and responsibilities

Subscribers must first authenticate with valid credentials before submitting a certificate request. Additionally, they must demonstrate their possession of the private key corresponding to the public key sent in the certificate request.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

The Apple IST CAs will perform the following identification and authentication steps:

- The certificate request came from valid Apple staff.
- The certificate request is for an authorized Apple owned domain.

4.2.2. Approval or rejection of certificate applications

Applications will be rejected for any of the following reasons:

- The certificate request is not from valid Apple staff.
- The certificate request is not for an authorized Apple owned domain.

4.2.3. Time to process certificate applications

Certificate requests are processed within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in a relevant Agreement.

4.3. Certificate Issuance

4.3.1. CA actions during certificate issuance

A certificate is created and issued following approval of the certificate application by an Apple IST CA. The CA will use the information provided in the Certificate Signing Request to issue the Certificate.

4.3.2. Notification to subscriber by the CA of issuance of certificate

Notification to Subscribers is deemed to have taken place when newly issued Certificates are downloaded to the Subscriber's machine.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

Certificates shall be deemed accepted and valid immediately after issuance.

4.4.2. Publication of the certificate by the CA

There is no public repository of Certificates.

4.4.3. Notification of certificate issuance by the CA to other entities

The Apple IST CAs do not provide notification of issuance to parties other than the Subscriber.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

Certificates use must be consistent with the permitted uses described in Section 1.4.1.

Subscriber responsibilities include:

- safeguarding their private key(s) from compromise
- promptly requesting that a certificate be revoked if the Subscriber has reason to believe that there has been a compromise of the Certificates associate

4.5.2. Relying party public key and certificate usage

Relying Parties are obligated to:

- Acknowledge that they are solely responsible for deciding whether or not to rely on the information in a Certificate, and agree that they have sufficient information to make an informed decision. Apple shall not be responsible for assessing the appropriateness of the use of a Certificate.
- Acknowledge that, to the extent permitted by applicable law, Apple hereby disclaims all warranties regarding the use of any Certificates, including any warranty of merchantability or fitness for a particular purpose. In addition, Apple hereby limits its liability, and excludes all liability for indirect, special, incidental, and consequential damages.
- Restrict reliance on Certificates issued by an Apple IST CA to the purposes for which those Certificates were issued, in accordance with Section 1.4.1 herein, and all other applicable sections of this CPS.

4.6. Certificate renewal

4.6.1. Circumstance for certificate renewal

Certificate renewal follows the same process as the initial issuance.

4.6.2. Who may request renewal

Only the Subscriber who requested the original certificate or an authorized representative may request certificate renewal.

4.6.3. Processing certificate renewal request

Certificate renewal requests are processed via the same process as initial issuance.

4.6.4. Notification of new certificate issuance to subscriber

Notification to Subscribers is deemed to have taken place when newly issued Certificates are downloaded to the Subscriber's machine.

4.6.5. Conduct constituting acceptance of a renewal certificate

Certificates shall be deemed accepted and valid immediately after issuance.

4.6.6. Publication of the renewal certificate by the CA

There is no public repository of Certificates.

4.6.7. Notification of certificate issuance by the CA to other entities

The Apple IST CAs do not provide notification of issuance to parties other than the Subscriber

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key

Certificate re-key requests follow the same process as for initial certificate issuance.

4.7.2. Who may request certification of a new public key

Only the Subscriber who requested the original certificate or an authorized representative may request certificate renewal.

4.7.3. Processing certificate re-keying requests

Certificate re-key requests are processed via the same process as initial issuance.

4.7.4. Notification of new certificate issuance to subscriber

Notification to Subscribers is deemed to have taken place when newly issued Certificates are downloaded to the Subscriber's machine.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

Certificates shall be deemed accepted and valid immediately after issuance.

4.7.6. Publication of the re-keyed certificate by the CA

There is no public repository of Certificates.

4.7.7. Notification of certificate issuance by the CA to other entities.

The Apple IST CAs do not provide notification of issuance to parties other than the Subscriber

4.8. Certificate modification

4.8.1. Circumstance for certificate modification

Subscribers may request certificate modification via the same process as for initial certificate issuance.

4.8.2. Who may request certificate modification

Only the Subscriber who requested the original certificate or an authorized representative may request certificate renewal.

4.8.3. Processing certificate modification requests

Certificate modification requests are processed via the same process as initial issuance

4.8.4. Notification of new certificate issuance to subscriber

Notification to Subscribers is deemed to have taken place when newly issued Certificates are downloaded to the Subscriber's machine.

4.8.5. Conduct constituting acceptance of modified certificate

Certificates shall be deemed accepted and valid immediately after issuance.

4.8.6. Publication of the modified certificate by the CA

There is no public repository of Certificates.

4.8.7. Notification of certificate issuance by the CA to other entities

The Apple IST CAs do not provide notification of issuance to parties other than the Subscriber

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

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

4.9.2. Who can request revocation

Only the Subscriber who requested the original certificate or an authorized representative may request certificate renewal.

4.9.3. Procedure for revocation request

The certificate revocation process will commence upon receipt of a valid request to revoke the set of Certificates from the Subscriber. The Subscriber will be required to authenticate. After authentication, the Subscriber will indicate that they wish to revoke their Certificate. Once a certificate has been revoked, its revocation status cannot be modified. An email is sent to the Subscriber to notify that the certificate has been revoked.

4.9.4. Revocation request grace period

There is no grace period within which the Subscriber must make a revocation request. Revocations can only be processed for certificates that have not been expired.

4.9.5. Time within which CA must process the revocation request

The Apple IST CAs take commercially reasonable steps to process revocation requests within 24 hours.

4.9.6. Revocation checking requirement for relying parties

Relying parties are solely responsible for performing revocation checking on Certificates before deciding whether or not to rely on the information in a Certificate.

4.9.7. CRL issuance frequency

CRLs are updated and issued at least every 7 days. Certificates remain in the CRL until the Certificates have expired.

4.9.8. Maximum latency for CRLs

CRLs will be updated before the existing CRL expiration date.

4.9.9. On-line revocation/status checking availability

OCSP is available via the URL noted in the Authority Information Access (“AIA”) extension in the Certificate.

4.9.10. On-line revocation status checking requirements

OSCP status requests must contain at a minimum the certificate serial number and Issuer DN to receive a valid response. Once an OCSP request has been validated, a signed response is sent to the requestor indicating the status of the Certificate and showing the request was successful. Failed OCSP requests will generate a failure status back to the requestor.

4.9.11. Other forms of revocation advertisements available

No other forms of revocation advertisements available.

4.9.12. Special requirements regarding key compromise

In the event of key compromise of the Sub-CA signing key, a decision will be made regarding the plan for the following:

- Provision of notice to related parties affected by the termination,
- The revocation of certificates issued by the Sub-CA,
- The preservation of the Sub-CAs archives and records

4.9.13. Circumstances for suspension

The Apple IST CAs do not support Certificate suspension.

4.10. Certificate status services

4.10.1. Operational characteristics

Certificate status services are available via the CRL URL or the OCSP URL noted in the Certificates.

4.10.2. Service Availability

The Apple IST CAs take commercially reasonable steps to provide certificate status services 24x7. .

4.10.3. Optional features

Not applicable.

4.11. End of subscription

A Subscriber may end subscription for a Certificate by allowing the certificate to expire without renewing the Certificate, or by revoking the certificate prior to expiration without replacing the Certificate.

4.12. Key escrow and recovery

4.12.1. TLS Client and Server Authentication

The Apple IST CAs do not provide key escrow and recovery services for these types of certificates.

5. Facility, management, and operational controls

5.1. Physical Controls

5.1.1. Site location and construction

Equipment supporting CA operations resides within a physically secured location in an Apple owned data center.

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 and CA facilities. Details of the physical security policies and procedures are in appropriate internal security documents.

5.1.3. Power and air conditioning

Equipment is protected to reduce risks from power and air conditioning disruption or failure.

5.1.4. Water exposures

Equipment is protected to reduce risks from water exposure.

5.1.5. Fire prevention and protection

Equipment is protected to reduce risks from fire.

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.

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.

5.2. Procedural controls

5.2.1. Trusted roles

Trusted Persons include all employees who are authorized to manage CA configurations and keys.

5.2.2. Number of persons required per task

Access to cryptographic hardware storing key material requires a minimum of two Trusted Persons.

5.2.3. Identification and authentication for each role

Trusted Persons must be Apple employees whose identity has been confirmed through background checking procedures and who have accepted the responsibilities of a Trusted Person.

5.2.4. Roles requiring separation of duties.

Key management operations must be performed under dual person control by Trusted Persons.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

Trusted persons are Apple personnel who have completed background checks and have demonstrated the skills and experience to accept the Trusted Person responsibilities.

5.3.2. Background check procedures

Before beginning employment as a Trusted Person, Apple performs background checks.

5.3.3. Training requirements

Employees are trained on Trusted Person roles and responsibilities before becoming a Trusted Person.

5.3.4. Retraining frequency and requirements

Trusted Persons are retrained as requirements and responsibilities are added, or modified.

5.3.5. Job rotation frequency and sequence

Not applicable.

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

Independent contractors will not be allowed to become a Trusted Person.

5.3.8. Documentation supplied to personnel

Trusted Person policies and procedures are posted in an internal site that is made available to all Trusted Persons.

5.4. Audit logging procedures

5.4.1. Types of events recorded

The Apple IST CAs record the following events:

- CA key lifecycle events such as CA key generation, storage, backup, and destruction.
- Certificate lifecycle management events such as certificate requests, issuance, and revocation.
- Security events such as system access attempts and CA facility entries and exits.

5.4.2. Frequency of processing log

Event logs are reviewed periodically for evidence of unauthorized activity.

5.4.3. Retention period for audit log

A risk assessment has been performed to determine the appropriate length of time for retention of archived event journals.

5.4.4. Protection of audit log

Audit logs are maintained securely within the CA facilities and is subject to the same degree of protection as the CA hardware.

5.4.5. Audit log backup procedures

Audit logs are archived and retained for the duration of the retention period described in 5.4.3.

5.4.6. Audit collection system (internal vs. external)

Not applicable.

5.4.7. Notification to event-causing subject

Not applicable.

5.4.8. Vulnerability assessments

The Apple IST CAs perform regular vulnerability assessments on CA supporting systems.

5.5. Records archival

5.5.1. Types of records archived

The Apple IST CAs archive the following types of records:

- Certificate lifecycle management events such as certificate requests, issuance, and revocation.
- Key lifecycle management events such as key generation, backup, archival, and destruction.

5.5.2. Retention period for archive

Records are retained for seven years.

5.5.3. Protection of archive

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

.

5.5.4. Archive backup procedures

Not applicable.

5.5.5. Requirements for time-stamping of records

Certificates, CRLs and other revocation entries shall contain date and time information.

5.5.6. Archive collection system (internal or external)

Not applicable.

5.5.7. Procedures to obtain and verify archive information

On a periodic basis, a sample of archived records will be restored to check the continued integrity and readability of the data.

5.6. Key changeover

Sub-CA key pairs are retired at the end of their lifetimes as defined in this CPS. If a CA needs to be renewed after the end of the key lifetime, a new CA keypair will be generated and a new certificate request will be made to obtain a new CA certificate.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

If a potential security incident or compromise is detected, an investigation will be performed to determine the degree and nature of the incident. A determination will be made as to whether Certificates will need to be revoked, and whether Subscribers and/or Relying parties need to be notified.

5.7.2. Computing resources, software, and/or data are corrupted

In the event that computing resource, software, and/or data is corrupted, appropriate escalation incident investigation, and response will commence.

5.7.3. Entity private key compromise procedures

In the event of compromise of a CA private key, incident handling procedures will be implemented and a risk analysis will be performed to determine whether all Certificates issued from the CA will be revoked.

5.7.4. Business continuity capabilities after a disaster

The Apple IST CAs have business continuity plans to maintain or restore business operations in a timely manner following interruption or failure of critical business processes.

5.8. CA or RA termination

Any decision to terminate an Apple IST CA shall be approved by the Policy Authority prior to the effective date of termination.

At the time of termination of the Sub-CA, Apple will develop a termination plan addressing the following:

- Provision of notice to related parties affected by the termination,
- The revocation of certificates issued by the Sub-CA,
- The preservation of the Sub-CA's archives and records

6. Technical Security Controls

6.1. Key pair generation and installation

6.1.1. Key pair generation

CA Signing key generation occurs using a secure cryptographic device meeting the requirements in Section 6.2.

Subscriber key pair generation is not currently supported.

6.1.2. Private key delivery to subscriber

Not applicable.

6.1.3. Public key delivery to certificate issuer

Delivery of a CA public key is submitted via a PKCS#10 Certificate Signing Request (CSR) to certificate issuance.

Public keys for Subscriber certificates issued by an Apple IST CA are submitted via a PKCS#10 Certificate Signing Request (CSR) after authentication with the appropriate credentials.

6.1.4. CA public key delivery to relying parties

The CA public key is provided as part of the CA Certificate that may be downloaded from www.apple.com/certificateauthority

6.1.5. Key sizes

Key pairs will be of the following minimum lengths:

- RSA-2048
- EC P-256

6.1.6. Public key parameters generation and quality checking

Certificate Signing Requests (CSRs) will be reviewed to confirm that the public key meets with minimum key sizes as defined in Section 6.1.5.

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

Key usages are defined in Section 7.1.

6.2. Private key protection and cryptographic module engineering controls

6.2.1. Cryptographic module standards and controls

Private keys are stored in a hardware security module (HSM) that certified at a minimum level of FIPS 140-2 level 3.

6.2.2. Private key (m of n) multi-person control

Private keys are protected with multi-person control which requires a minimum of two Trusted Persons.

6.2.3. Private key escrow

Private keys are backed up but not escrowed.

6.2.4. Private key backup

Private keys are backed up to cryptographic devices under the same multi-person control as the original private key.

6.2.5. Private key archival

Archived keys are securely stored using offline media under multi-person control.

6.2.6. Private key transfer into or from a cryptographic module

Private key transfer into or from a cryptographic module is done in accordance to manufacturer's guidelines and under multi-person control.

6.2.7. Private key storage on cryptographic module

Private keys are stored in a hardware security module (HSM) that is tamper resistant and certified at a minimum level of FIPS 140-2 level 3.

6.2.8. Method of activating private key

Activation of CA private keys is done in accordance with the instructions and documentation provided by the manufacturer of the hardware security module and performed by Trusted Persons.

6.2.9. Method of deactivating private key

Private keys are deactivated upon executing a deactivation command or system power off .

6.2.10. Method of destroying private key

Private keys on cryptographic devices will be destroyed in accordance with instructions and documentation provided by the manufacturer.

6.2.11. Cryptographic module rating

Hardware security modules are certified at a minimum level of FIPS 140-2 level 3.

6.3. Other aspects of key pair management

6.3.1. Public key archival

Not applicable.

6.3.2. Certificate operational period and key pair usage periods

Operational period for key pairs is the same as the operational period for associated certificates.

Certificates issued from an Apple IST CA shall not be valid for longer than 39 months.

6.4. Activation data

6.4.1. Activation data generation and installation

Private keys are required to be protected using strong passwords.

6.4.2. Other aspects of activation data

Not applicable.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

The following computer security components are in place for systems supporting the CA:

- Physical security and environment controls (see Section 5.1 of this CPS)
- System development controls (see Section 6.6 of this CPS)
- Trusted Person controls (see Section 5.2 of this CPS)
- Logical access controls including event logging (see Section 5.4 of this CPS)

6.5.2. Computer security rating

Not applicable.

6.6. Life cycle technical controls

6.6.1. System development controls

Changes to software or hardware supporting the production Sub-CAs are tested and approved by management prior to implementation.

6.6.2. Security management controls

System configurations are periodically reviewed to identify any unauthorized changes.

6.6.3. Life cycle security controls

Not applicable.

6.7. Network security controls

Network security measures are in place to protect against denial of service and intrusion attacks. Access controls lists are configured to deny all but the necessary services to support the CA systems.

6.8. Time-stamping

CA systems are regularly synchronized with a reliable time service. Certificates, CRLs and other revocation entries shall contain date and time information.

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate profile

TLS Server and Client Certificates

TLS Server and Client certificates issued from an Apple IST CA shall conform to the X.509 Certificate format and contain at a minimum, the following data elements

Field/Attribute	Critical	Value
Signature Algorithm	N/A	RSA-SHA256 or ECDSA-SHA256
Key Usage	Yes	Digital Signature, Key Encipherment (for RSA keys) or Key Agreement (for EC keys)
Extended Key Usage	Yes	Server Authentication (1.3.6.1.5.5.7.3.1) and/or Client Authentication (1.3.6.1.5.5.7.3.2)
Basic Constraints	Yes	Certification Authority = No
Certificate Policies	No	(1.2.840.113635.100.5.11.4)

7.2. CRL profile

A CRL issued by an Apple IST CA shall conform to the X.509 version 2 CRL format. Each CRL shall contain the following fields:

- Signature Algorithm using SHA-2 with RSA, or SHA-2 with ECDSA
- Issuer matching the Apple IST CA Certificate's Distinguished Name
- "Last Update" field with the time of CRL issuance
- "Next Update" field defining the period of validity
- Authority Key Identifier extension
- List of Revoked Certificates

7.3. OCSP profile

OCSP responses conform with RFC 2560, Version 1. OCSP responses will include the following fields:

- Signature algorithm using at least SHA-2 with RSA, or SHA-2 with ECDSA
- The OCSP responder certificate
- "Produced at" time indicating when the response was signed
- Certificate status (good/revoked/unknown)
- "This Update" field with the time of OCSP response issuance
- "Next Update" field defining the period of validity

8. Compliance audit and other assessments

8.1. Frequency or circumstances of assessment

An annual audit will be performed by an independent external auditor to assess the adequacy of the business practices disclosure and compliance of the CA's controls to one or more of the following standards:

- AICPA/CICA Trust Service Principles and Criteria for Certification Authorities
- AICPA/CICA WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria

8.2. Identity/qualifications of assessor

The auditors performing an annual audit shall be from an independent audit firm that is approved to audit according to AICPA/CICA WebTrust for Certification Authorities principles and criteria.

8.3. Assessor's relationship to assessed entity

Apple will retain the external audit firm, and individual auditors shall not be employees or related to employees of Apple.

8.4. Topics covered by assessment

The audit will meet the requirements of the audit schemes identified in Section 8.1.

8.5. Actions taken as a result of deficiency

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

8.6. Communication of results

Audit results shall be communicated to the CA Management Team and may be communicated to the others as deemed appropriate.

A copy of the latest WebTrust for CA audit report can be found at www.apple.com/certificateauthority.

9. Other business and legal matters

9.1. Fees

9.1.1. Certificate issuance or renewal fees

No fees are charged for this service.

9.1.2. Certificate access fees

No fees are charged for this service.

9.1.3. Revocation or status information access fees

No fees are charged for this service.

9.1.4. Fees for other services

No fees are charged for CA services.

9.1.5. Refund policy

Not applicable.

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 an Apple IST CA.

9.2.1. Insurance coverage

Not applicable.

9.2.2. Other Assets

Not applicable.

9.2.3. Insurance or warranty coverage of end-entities

Not applicable.

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

The Apple IST CAs shall keep the following information confidential at all times:

- Private signing and client authentication keys
- Personal or non-public information about Subscribers
- Security mechanisms

9.3.2. Information not within the scope of confidential information

The following information shall not be considered confidential:

- Information included in Certificates
- Apple IST CA public Certificates
- Information contained in this CPS document
- Any Certificate status or Certificate revocation reason code

9.3.3. Responsibility to protect confidential information

Except as required to support the audits performed by an independent external audit firm, confidential information should not be released to third parties unless required by law or requested by a court with jurisdiction over the CA. The information will be kept confidential even after the termination of the CA.

9.4. Privacy of personal information

9.4.1. Privacy plan

Not applicable as all Subscribers are internal to Apple.

9.4.2. Information treated as private

Any information that is not publicly available through the content of the issued certificate, and online CRLs is treated as private.

9.4.3. Information not deemed private

Any information publicly available through a certificate is not deemed private.

9.4.4. Responsibility to protect private information

Not applicable as all Subscribers are internal to Apple.

9.4.5. Notice and consent to use private information

Not applicable as all Subscribers are internal to Apple.

9.4.6. Disclosure pursuant to judicial or administrative process.

Not applicable as all Subscribers are internal to Apple.

9.4.7. Other information disclosure circumstances

Not applicable as all Subscribers are internal to Apple.

9.5. Intellectual property rights

Certificates and CRLs issued by the Apple IST CAs, information provided via OCSP, and this CP/CPS are the property of Apple.

9.6. Representations and warranties

9.6.1. CA representations and warranties.

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

9.6.2. RA representations and warranties

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

9.6.3. Subscriber representations and warranties

Not applicable. There are no Subscriber warranties as all Subscribers are internal to Apple.

9.6.4. Relying party representations and warranties

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

9.6.5. Representations and warranties of other participants

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

9.7. Disclaimers of warranties

To the extent permitted by applicable law any applicable Relying Party Agreements shall disclaim any warranties, including any warranty of merchantability or fitness for a particular purpose on behalf of Apple.

9.8. Limitations of liability

To the extent permitted by applicable law, Apple shall not be held liable for any direct, indirect, special, incidental, and consequential damages.

9.9. Indemnities

There is no Subscriber indemnity as all Subscribers are internal to Apple.

To the extent permitted by law, each Relying Party shall indemnify Apple, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10. Term and termination

9.10.1. Term

The CPS and/or Relying Party Agreement become effective upon publication to www.apple.com/certificateauthority. Amendments to this CPS and Relying Party Agreement become effective upon publication to www.apple.com/certificateauthority.

9.10.2. Termination

This CPS and/or Relying Party Agreement shall remain in force until terminated or replaced by a new version.

9.10.3. Effect of termination and survival

Upon termination of this CPS and/or Relying Party Agreement, Apple IST PKI Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11. Individual notices and communications with participants

The latest CPS and/or Relying Party Agreement is made publicly available at www.apple.com/certificateauthority.

9.12. Amendments

9.12.1. Procedure for amendment

This CPS and/or Relying Party Agreement may be amended at any time without prior notice. The latest CPS is made publicly available at www.apple.com/certificateauthority.

9.12.2. Notification mechanism and period

The latest CPS is made publicly available at www.apple.com/certificateauthority.

9.12.3. Circumstances under which OID must be changed

Not applicable.

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.

9.14. Governing law

The terms in this CPS are governed by and construed in accordance with the laws of the United States and the State of California, except that body of California law concerning conflicts of law.

9.15. Compliance with applicable law

Please refer to Section 9.14.

9.16. Miscellaneous provisions

9.16.1. Entire agreement
See applicable Relying Party Agreement.

9.16.2. Assignment
See applicable Relying Party Agreement.

9.16.3. Severability
See applicable Relying Party Agreement.

9.16.4. Enforcement (attorneys' fees and waiver of rights)
See applicable Relying Party Agreement.

9.16.5. Force Majeure
See applicable Relying Party Agreement.

9.17. Other provisions
Not applicable.