Apple Inc.

Certification Practice Statement
Apple Public CA

Version 4.3

Effective Date: April 01, 2020

Table of Contents

1. INTRODUCTION

1.1. OVERVIEW

This Certification Practice Statement ("CPS") describes the practices employed by Apple acting as a publicly-trusted Certification Authority ("Apple Public CA") in issuing and managing digital certificates, used to secure connections based on the TLS protocol, for S/MIME, and related services.

The Apple Public CA is issued Certificates by publicly-trusted Root Certification Authorities that are widely trusted by suppliers of Internet browser software or other relying-party application software. As such, the Apple Public CA inherits the benefits and responsibilities associated with the public trust from the issuing Public Root Certification Authorities.

This CPS further defines the practices 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.

This document specifies the policies Apple Inc. adopts to meet the current versions of the following policies, guidelines, and requirements:

Name of Policy/ Guideline/ Requirement Standard	Location of Source Document
The Certification Authority / Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly- Trusted Certificates ("Baseline Requirements")	https://cabforum.org/baseline-requirements-documents/
The CAB Forum Network and Certificate System Security Requirements	https://cabforum.org/network-security-requirements/
Mozilla Root Store Policy	https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
Apple Root Store Program	https://www.apple.com/certificateauthority/ca_program.html
DigiCert Certificate Policy	https://www.digicert.com/wp-content/uploads/2020/03/DigiCert-CP-v5.1.pdf

1.2. DOCUMENT NAME AND IDENTIFICATION

This is the Apple Public CA CPS. The name reflects the publicly-trusted nature of the Certification Authority regulated by this CPS, and supersedes the prior name "Apple IST CPS".

TLS Certificates regulated by this CPS are issued with at least one Certificate Policy object identifier shown below to assert that Apple makes commercially reasonable efforts to conform to the latest version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates published at http://www.cabforum.org.

Policy Object Identifier Description	Policy OID
appleCABFSSLBaselineCertificatePolicy	1.2.840.113635.100.5.11.4 (Mandatory)
ca-browser-forum-organization-validated	2.23.140.1.2.2 (Optional)

S/MIME Certificates regulated by this CPS are issued with the following Certificate Policy object identifier values:

Policy Object Identifier Description	Policy OID
Secure Email Only - Sign and Encrypt	1.2.840.113635.100.5.11.5.1
Secure Email Only - Sign	1.2.840.113635.100.5.11.5.2
Secure Email Only - Encrypt	1.2.840.113635.100.5.11.5.3
Future Use	1.2.840.113635.100.5.11.5.4
Future Use	1.2.840.113635.100.5.11.5.5
Future Use	1.2.840.113635.100.5.11.5.6
Future Use	1.2.840.113635.100.5.11.5.7
Future Use	1.2.840.113635.100.5.11.5.8
Future Use	1.2.840.113635.100.5.11.5.9

The Apple Public CA CPS is reviewed and updated at least annually, as required by the Baseline Requirements. It is structured according to RFC 3647; the words "No Stipulation" are applied to section headings if the Apple Public CA imposes no requirements related to that section.

1.2.1. Revisions

The following revisions have been made to the original document:

Date	Changes	Version
04/01/2020	Updated the document to meet requirements of version 2.7 of the Mozilla Root Store Policy. Completed annual review as required by the Baseline Requirements. Incorporated content from the Apple Corporate Email CPS version 2.3 dated 06/05/2019.	4.3

06/14/2019	Updated contact information in section 1.5.2 and made minor changes to section 4.1.1 and 4.9.2.	4.2
05/31/2019	Removed deprecated Domain Authorization validation method in section 3.2.2.1.	4.1
12/11/2018	Modified section 1.1 to introduce the concept of Apple Public CA and removed references to Apple IST CA throughout the document. Modified section 1.2 to introduce a new document name. Added the Organization Validated optional policy object identifier from the Baseline Requirements. Updated contact information in section 1.5.2. Added section 3.1.1.2 to include a new Sub-CA Certificate naming schema valid starting on December 11, 2018. Added section 3.2.2.1 to specify the methods used for validation of authorization of control.	4.0
03/01/2018	Updated section 6.3.2 to conform with CAB Forum ballot 193 – 825-day Certificate Lifetimes. Added definition for Certificate Transparency, and CT and TLS acronyms in section 1.6. Added the SCT extension to profiles in section 7.1.	3.4
09/06/2017	Removed reference to IST CA 6 in section 1.1. Updated definitions and acronyms in sections 1.6 to include CAA. Updated section 4.2.1 to conform with CAB Forum ballot 187 - Make CAA Checking Mandatory. Updated font to SF Hello Thin. Updated references of WebTrust governing body to CPA Canada.	3.3
12/01/2016	Added references to the specific CAs covered in the CPS: IST CA 3, and IST CA 6.	3.2
08/15/2016	Added references to the specific CAs covered in the CPS: IST CA 2, IST CA 4, and IST CA 8.	3.1

01/28/2016	Updates to clarify that CAA records are not reviewed. Clarifications on the scope of cryptographic module engineering controls. Minor grammatical updates.	3.0
02/16/2015	Updates for conformance with SSL Baseline Requirements for Publicly Trusted Certificates.	2.0
08/25/2014	Initial release.	1.0

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

This is an entity that is authorized to issue, manage, revoke, and renew Certificates. Apple acts as the Certification Authority.

1.3.2. Registration Authorities

The Registration Authority performs identification and authentication checks for end-user certificate applicants. Apple acts as the Registration Authority. This function is not delegated to a third party.

1.3.3. Subscribers

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

1.3.4. Relying Parties

This is any entity that receives an X.509 certificate (issued to a subscriber by the Apple Public 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 Public CA issues and administers 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.

1.4.1.2. S/MIME Certificates

The Apple Public CA issues and administers X.509 Certificates with an Email Protection Extended Key Usage (EKU) used to provide secure email. This type of Certificate may be used to digitally sign an email message from an authorized apple.com or filemaker.com email account, and/or encrypt a message to an authorized apple.com or filemaker.com email account, prior to delivery. For avoidance of doubt, emails associated with a S/MIME Certificate are not intended to replace a written signature or eSignature. S/MIME Certificates are only intended to indicate that the email is from an authorized apple.com or filemaker.com email account, and does not provide any assurance of the identity of the sending party.

1.4.2. Prohibited Certificate Uses

The Apple Public CA does 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 Public 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 Apple Public 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
One Apple Park Way
Cupertino, CA 95014

(408) 996-1010
policy_authority@apple.com

To submit a Certificate Problem Report, there are two mechanisms:

- Relying Parties, Application Software Suppliers, and other third parties contact us at contact_pki@apple.com.
- Subscribers as they are internal to Apple, use mechanisms available through the Certificate issuing application.

1.5.3. Person Determining CPS Suitability for the Policy

The Apple CA Policy Authority determines the suitability and applicability of this CPS based on the results and observations received from an independent auditor (see Section 8).

1.5.4. CPS Approval Procedures

This CPS and all amendments to this CPS are 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 (see Section 1.2.1), except where the amendments are purely clerical.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

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.
Certification Authority Authorization	As defined by RFC 6844, the Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain.
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 Public CA.
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.
Certificate Transparency	A protocol for publicly logging the existence of TLS Certificates as they are issued or observed, in a manner that allows anyone to audit Certificate Authority activity and notice the issuance of suspect Certificates as well as to audit the certificate logs themselves.
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 the Apple Public CA) and has an interest of some kind in the validity of the certificate.
Repository	As used, same as Directory.
Root Certification Authority or Root CA	This is a CA that is at the top of a hierarchical PKI network.
Subscriber	This is an entity who has been issued a Certificate signed by an Apple Public CA Certificate. All Subscribers are internal to Apple.
Subordinate Certification Authority or Sub-CA	This is a CA that is a node of the Root CA within a hierarchical PKI network.
S/MIME	S/MIME (Secure/Multipurpose Internet Mail Extensions) is a widely accepted method (or more precisely, a protocol) for sending digitally signed and encrypted messages.

1.6.2. 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
CAMT	Certification Authority Management Team
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CT	Certificate Transparency
FQDN	Fully Qualified Domain Name
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
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

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

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 the Apple Public 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>

3.1.1.2. S/MIME Certificates

Field/Attribute	Value
Country (C)	US
State (ST)	California
Organization (O)	Apple Inc.
Common Name	<rfc822Name with a domain-part equal to either apple.com or filemaker.com>

3.1.1.3. TLS Server Sub-CA Certificates

Sub-CA Certificates will conform to one of the Subject Distinguished Name structures below.

Field/Attribute	Value
Country (C)	US
State (ST)	California
Organization (O)	Apple Inc.
Common Name	Apple IST CA [*number*] – G1

Field/Attribute	Value
Country (C)	US

State (ST)	California
Organization (O)	Apple Inc.
Common Name	Apple Public Server [*technology*] CA [*number*] – G[*generation*]

Technology: A string representing the technology used for issued Certificates. For example, "ECC" or "RSA".

Number: A numeric value that uniquely distinguishes the CA from others.

Generation: A numeric value that starts with one (1) and increases by one (1) when a new Certificate is issued under a particular "number".

3.1.1.4. S/MIME Sub-CA Certificates

Sub-CA Certificates will conform to one of the Subject Distinguished Name structures below.

Field/Attribute	Value
Country (C)	US
State (ST)	California
Organization (O)	Apple Inc.
Common Name	Apple IST CA [*number*] – G1

Field/Attribute	Value
Country (C)	US
State (ST)	California
Organization (O)	Apple Inc.
Common Name	Apple Public Client [technology] CA [number] – G[generation]

Technology: A string representing the technology used for issued Certificates. For example, "ECC" or "RSA".

Number: A numeric value that uniquely distinguishes the CA from others.

Generation: A numeric value that starts with one (1) and increases by one (1) when a new Certificate is issued under a particular "number".

3.1.2. Need for Names To Be Meaningful

When applicable, the Apple Public CA shall use distinguished names to identify both the entity that is the subject of the Certificate and the entity that is the issuer of the Certificate.

3.1.3. Anonymity Or Pseudonymity Of Subscribers

No Stipulation.

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

The uniqueness of each subject name in a Certificate is enforced as follows:

Certificate Type	Uniqueness Determination
TLS Certificate	Inclusion of the domain name in the Certificate. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).
S/MIME Certificate	Requiring a unique email address combined/associated with a unique serial integer.

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 and Domain Identity

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

3.2.2.1. Validation of Domain Authorization or Control

Prior to issuance of a TLS Certificate, the Apple Public CA validates each Fully Qualified Domain Name to be included in such Certificate. Effective on May 31, 2019, the validation of FQDNs is carried out using only the method described in the Baseline Requirements section 3.2.2.4.2.

3.2.3. Authentication of Individual Identity

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

3.2.4. 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 Apple Public 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. Verification of Domain Name Ownership

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

3.2.7. Criteria for Interoperation

No Stipulation.

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.

3.4. 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 active 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 Public CA will verify that:

- The certificate request came from Apple staff,
- The certificate request is for an authorized Apple owned domain or email address,
- A CAA record check is performed against each FQDN in the TLS Certificate request.

The CAA record verifies the presence of "pki.apple.com" in either the 'issue' or 'issuewild' properties for each FQDN provided. The 'iodef' property is checked but no action will be taken. The following criteria will be used to establish whether to issue the certificate:

- If the CAA record is not present in DNS, the certificate will be issued.
- If the 'issue' and 'issuewild' properties are empty or list the name "pki.apple.com" as an authorized CA, the certificate will be issued.
- If the 'issue' or 'issuewild' properties list a name other than "pki.apple.com" as an authorized CA, the certificate will not be issued.
- In any other cases, the certificate will not be issued.

The CAA check will be performed immediately before the issuance of the certificate, but does not exclude the possibility of other CAA checks.

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.

- The certificate request is not for an authorized Apple email address.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 the Apple Public CA. The Apple Public CA will use the information provided in the Certificate Signing Request to issue the Certificate.

For S/MIME Certificates:

- The issuance is contingent upon the requesting Subscriber having an authorized apple.com or filemaker.com email account.
- The Subscriber requests a certificate via authentication with the appropriate credentials. Once the request is confirmed to be for an authorized apple.com or filemaker.com email account, a Certificate may be issued. Certificates and keys are provided to the Subscriber via a secure mechanism.

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

In General, notification to Subscribers is deemed to have taken place when newly issued Certificates are downloaded to the Subscriber's machine.

Upon issuance of a S/MIME Certificate, the Apple Public CA will notify the Subscriber by sending notice to the email address in the Subscriber certificate.

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 Public CA does 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 the Apple Public 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 Requests

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 Public CA does 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.

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

The Apple Public CA does 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 Public CA does not provide notification of issuance to parties other than the Subscriber.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

Apple reserves the right to revoke any Certificates, without notice, if it believes the Subscriber's private key has been compromised, or upon request from the Subscriber.

4.9.1.1. Reasons for Revoking a Subscriber Certificate

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

TLS Certificates

The Apple Public CA takes commercially reasonable steps to revoke a TLS Certificate within 24 hours after confirming one or more of the following occurred:

1. The Subscriber requests in writing that the Apple Public CA revoke the TLS Certificate;
2. The Subscriber notifies the Apple Public CA that the original TLS Certificate request was not authorized and does not retroactively grant authorization;

3. The Apple Public CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the TLS Certificate suffered a Key Compromise; or

4. The Apple Public CA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the TLS Certificate should not be relied upon.

The Apple Public CA may revoke a TLS Certificate within 24 hours and will take commercially reasonable steps to revoke a TLS Certificate within 5 days after confirming that one or more of the following occurred:

1. The TLS Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the Baseline Requirements or any section of the Mozilla Root Store policy;

2. The Apple Public CA obtains evidence that the TLS Certificate was misused;

3. The Apple Public CA confirms that a Subscriber has violated one or more of its material obligations under any relevant agreement.

4. The Apple Public CA confirms any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the TLS Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

5. The Apple Public CA confirms that a TLS Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;

6. The Apple Public CA confirms a material change in the information contained in the TLS Certificate;

7. The Apple Public CA confirms that the TLS Certificate was not issued in accordance with the Baseline Requirements or the CPS;

8. The Apple Public CA confirms that any of the information appearing in the TLS Certificate is inaccurate;

9. The Apple Public CA's right to issue TLS Certificates under the Baseline Requirements expires or is revoked or terminated, unless the Apple Public CA has made arrangements to continue maintaining the CRL/OCSP Repository;

10. Revocation is required by the governing CP and/or the CPS; or

11. The Apple Public CA confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

S/MIME Certificates

The Apple Public CA takes commercially reasonable steps to revoke a S/MIME Certificate after confirming one or more of the following occurred:

1. The Subscriber indicates that the original Certificate request was not authorized and does not retroactively grant authorization;
2. The Apple Public CA obtains reasonable evidence that the Subscriber's private key (corresponding to the public key in the Certificate) has been compromised or is suspected of compromise;
3. The Apple Public CA obtains reasonable evidence that the Certificate has been used for a purpose outside of that indicated in the certificate or in the CA's subscriber agreement;
4. The Apple Public CA receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under an applicable subscriber agreement;
5. The Apple Public CA receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the Certificate is no longer legally permitted;
6. The Apple Public CA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
7. A determination that the Certificate was not issued in accordance with the Apple Public CA's CPS;
8. The Apple Public CA determines that any of the information appearing in the Certificate is not accurate;
9. The Apple Public CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
10. The Apple Public CA private key used in issuing the Certificate is suspected to have been compromised;
11. Such additional revocation events as the Apple Public CA publishes in its policy documentation; or

12. The Certificate was issued in violation of the then-current version of the MozillaRoot Store Policy requirements.

4.9.2. Who Can Request Revocation

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

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.

If the revocation of an Apple Public CA certificate chaining up to a root in Mozilla's root program is due to a security concern, a security bug will be filed in Bugzilla.

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 expired.

4.9.5. Time Within Which CA Must Process the Revocation Request

The Apple Public CA takes 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 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 Related to 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,
- A bug will be filed with Mozilla's Bugzilla.

4.9.13. Circumstances for Suspension

The Apple Public 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

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

Certificate status information for Subscriber Certificates is published via OCSP at least every four days and via CRL at least every seven days.

OCSP responses conform to the following:

- Do not respond with a "good" status for Certificates that have not been issued,
- Have a maximum expiration time of no more than 10 days.

CRLs conform to the following:

- Updated at least once every seven days,

- nextUpdate is no more than 10 days beyond the value of thisUpdate.

4.10.2. Service Availability

The Apple Public CA takes commercially reasonable steps to provide certificate status services 24x7.

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 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. Key Escrow and Recovery Policy and Practices

The Apple Public CA does not provide key escrow and recovery services for TLS Certificates.

Subscriber private keys for S/MIME Certificates are escrowed in an encrypted format. Escrowed keys can only be recovered after confirming the authority of the party requesting the private key.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No Stipulation.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL 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.

5.1.8. Off-Site Backup

Backups are taken at regular intervals and stored at alternate locations. For purposes of backup and recovery, Root CA and Sub-CA private keys, which are stored in encrypted form, are moved to secure storage under dual control. The backups exist in multiple copies in different geo locations.

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

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

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 Public CA records 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)

No Stipulation.

5.4.7. Notification To Event-Causing Subject

No Stipulation.

5.4.8. Vulnerability Assessments

The Apple Public CA performs regular vulnerability assessments on CA supporting systems

5.5. RECORDS ARCHIVAL

5.5.1. Types of Records Archived

The Apple Public CA archives 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

No Stipulation.

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)

No Stipulation.

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 Certificate 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

Business continuity plans have been developed to maintain or restore the Sub-CA business operations in a timely manner following interruption or failure of critical business processes.

5.8. CA OR RA TERMINATION

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

At the time of termination of the Apple Public 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 CA,
- The preservation of the 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 for TLS Certificates is not currently supported.

CAs that issue S/MIME Certificates generate a Subscriber key pair and the corresponding public certificate. The key pair may be used to sign and/or encrypt an email message.

6.1.2. Private Key Delivery to Subscriber

No stipulation for TLS Certificates. For S/MIME certificates, the key pair is provided securely to the Subscriber via a secure mechanism.

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 the Apple Public 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

CA 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 (n out of m) Multi-Person Control

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

6.2.3. Private Key Escrow

CA private keys are backed up but not escrowed.

6.2.4. Private Key Backup

CA 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

CA 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

CA 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

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

6.2.10.Method of Destroying Private Key

CA 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

No Stipulation.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

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

Certificates issued by the Apple Public CA on or after March 1, 2018, will not be valid for longer than 825 days.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

Private keys are required to be protected using strong passwords. Multi-factor authentication is enforced for access to administrative functions in the CA Software.

6.4.2. Activation Data Protection

Apple protects data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms.

6.4.3. Other Aspects of Activation Data

No Stipulation.

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

No Stipulation.

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

No Stipulation.

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

Apple Public CA Certificates

Apple Public CA certificates shall conform to the X.509 Certificate format.

An Apple Public CA certificate is deemed as capable of being used to issue new Subscriber certificates if it contains an X.509v3 basicConstraints extension with the cA boolean set to true.

Apple Public CA Certificates created after January 1, 2019 for issuance of publicly trusted certificates must contain an EKU extension; and must not include the anyExtendedKeyUsage KeyPurposeId; and, must not include both the id-kp-serverAuth and id-kp-emailProtection KeyPurposeIds in the same certificate.

Technically Constrained Apple Public CA Certificates shall include an Extended Key Usage (EKU) extension specifying all extended key usages for which the CA is authorized to issue certificates.

TLS Server and Client Certificates

TLS Server and Client Certificates issued by the Apple Public CA shall conform to the X.509 Certificate format and contain at a minimum, the following data elements:

Field/Attribute	Critical	Value
Serial Number	N/A	Certificate serial numbers are non-sequential and greater than zero (0) containing at least 64 bits of output from a CSPRNG.
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	appleCABFSSLBaselineCertificate Policy (1.2.840.113635.100.5.11.4) Mandatory ca-browser-forum-organization-validated (2.23.140.1.2.2) Optional

Certificates published to Certificate Transparency logs will include the following extension:

Field/Attribute	Critical	Value
Signed Certificate Timestamp	No	At least one Signed Certificate Timestamp

S/MIME Certificates

S/MIME Certificates issued by the Apple Public CA shall conform to the X.509 Certificate format and contain at a minimum, the following data elements:

Field/Attribute	Critical	Value
Serial Number	N/A	Certificate serial numbers are non-sequential and greater than zero (0) containing at least 64 bits of output from a CSPRNG.
Signature Algorithm	N/A	RSA-SHA256
Key Usage	Yes	Digital Signature, Key Encipherment
Extended Key Usage	Yes	Email Protection
Basic Constraints	Yes	Certification Authority = No
Subject Alternative Name	No	rfc882Name
Certificate Policies	No	1.2.840.113635.100.5.11.5.1

7.2. CRL PROFILE

A CRL issued by the Apple Public 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 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

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 Apple's business practices disclosure and compliance with this CPS for all CAs technically capable of issuing publicly trusted certificates.

For TLS Certificates, the auditor will also assess controls to the following standards:

- CPA Canada Trust Service Principles and Criteria for Certification Authorities
- CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

For S/MIME Certificates, the auditor will also assess controls to the following standard:

- CPA Canada Trust Service Principles and Criteria for Certification Authorities

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 CPA Canada WebTrust for Certification Authorities principles and criteria.

WebTrust auditors must meet the requirements of Section 8.2 of the CA/Browser Baseline Requirements.

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.

Copies of the latest audit reports can be found at www.apple.com/certificateauthority.

8.7. SELF-AUDITS

On at least a quarterly basis, Apple performs regular internal audits against TLS Certificates issued since the last internal audit.

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

No Stipulation.

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 Public CA.

9.2.1. Insurance Coverage

No Stipulation.

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 Apple Public CA 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
- 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

No Stipulation 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

No Stipulation as all Subscribers are internal to Apple.

9.4.5. Notice and Consent To Use Private Information

No Stipulation as all Subscribers are internal to Apple.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

No Stipulation as all Subscribers are internal to Apple.

9.4.7. Other Information Disclosure Circumstances

No Stipulation as all Subscribers are internal to Apple.

9.5. INTELLECTUAL PROPERTY RIGHTS

Certificates and CRLs issued by the Apple Public CA, 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

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, 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.

If the Apple Public CA fails to comply with the Mozilla Root Store Policy, the event will be classified as an incident and will be reported to Mozilla in the form of an Incident Report and updated regularly until the the corresponding bug is marked as resolved in the mozilla.org Bugzilla system by a Mozilla representative.

Additionally, any changes that are motivated by a security concern such as a certificate misissuance or a compromise of an Apple Public CA will be treated as a security incident and a bug will be filed in Bugzilla.

Apple will notify Mozilla if:

1. Ownership or control of the CA certificates changes;

2. An organization other than the CA obtains control of an unconstrained intermediate certificate (as defined in section 5.3.2 of the Mozilla Root Store policy) that directly or transitively chains to included certificate(s);

3. Ownership or control of Apple's operations changes; or

4. There is a material change in Apple's operations

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

No Stipulation.

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.

9.16.1.Force Majeure

See applicable Relying Party Agreement.

9.17. OTHER PROVISIONS

No Stipulation.