Apple Inc.
Certification Authority
Certification Practice Statement
Software Update

Version 1.3
Effective Date: April 26, 2018

Table of Contents

1. Introduction

This Certification Practice Statement ("CPS") describes the practices employed by the Software Update Subordinate Certification Authority ("Software Update Sub-CA," or "the Sub-CA") in issuing and managing digital Certificates and related services. These practices, and the structure of this document, are designed to align to the requirements defined in the Apple Certificate Policy ("CP").

1.1. Trademarks

Apple® is a trademark of Apple Inc., registered in the United States and other countries.

1.2. Table of acronyms

Please refer to the CP for a table of acronyms used within this document.

1.3. Definitions

Please refer to the CP for a table of definitions used within this document.

2. General business practices

This section establishes and sets forth the general business practices of the Software Update Sub-CA.

2.1. Identification

The practices set forth in this CPS apply exclusively to the Software Update Sub-CA. This CPS is structured similarly to the CP, disclosing details of the practices employed by the Software Update Sub-CA that address the more general requirements defined in the CP.

This document assumes that the reader is familiar with the general concepts of digital signatures, Certificates, and public-key infrastructure. If the reader is new to Public Key Infrastructure concepts, the reader may choose to consult the introduction and overview of the WebTrust Program for Certification Authorities, a guide published by the American Institute of Certified Public Accountants (AICPA) and freely available for download from their web site, www.aicpa.org. The guide contains an overview of PKI, including an orientation on key concepts such as digital signatures, asymmetric key pairs, certification authorities, registration authorities, policy and practice statements, and business issues and considerations.

For the purposes of this CPS, the term "Apple PKI" refers collectively to Apple PKI Service Providers and End Entities. Apple PKI Service Providers consist of (1) Apple Certification Authorities ("CAs"), including the Apple Root CA and the Software Update Sub-CA, and their related management teams that generate, issue, distribute, revoke and manage cryptographic keys and Certificates, (2) Apple Registration Authorities ("Apple RA"), and (3) the Apple CA Policy Authority ("Apple PA," or "PA"). End Entities consist of (1) Subscribers of Certificates and (2) Relying Parties who agree to be bound by the conditions set forth in this CP and any applicable CPS.

The Software Update Sub-CA issues and administers Certificates in accordance with policies in the CP.

2.2. Community and applicability

This CPS is applicable to the following Certificates issued by the Software Update Sub-CA:

- Software Update Signing Certificates: This type of Certificate may be used to digitally sign software packages in order to authenticate the source of the software package as Apple, and validate the integrity of the software package (it is complete and unaltered).

2.3. Contact details

The CA's Certificate Policies are administered by the Apple PA. The contact information for this CPS is:

Apple CA Policy Authority
C/O General Counsel
Apple Inc.
One Apple Park Way
Cupertino, California 95014

(408) 996-1010
policy_authority@apple.com

2.4. Apportionment of liability

This section is not applicable because the Software Update Sub-CA will be used internally by Apple to perform its own verification of software updates.

2.4.1. Warranties to Subscribers and Relying Parties

The Software Update Sub-CA does not have subscriber or relying party agreements, as all Subscribers and Relying Parties are internal to Apple.

2.4.2. CA disclaimers of warranties

The Software Update Sub-CA does not have subscriber or relying party agreements, as all Subscribers and Relying Parties are internal to Apple.

2.4.3. CA limitations of liability

The Software Update Sub-CA does not have subscriber or relying party agreements, as all Subscribers and Relying Parties are internal to Apple.

2.4.4. Subscriber warranties

The Software Update Sub-CA does not have subscriber or relying party agreements, as all Subscribers and Relying Parties are internal to Apple.

2.4.5. Private key compromise

The Software Update Sub-CA does not have subscriber or relying party agreements, as all Subscribers and Relying Parties are internal to Apple.

2.4.6. Relying Party liability

The Software Update Sub-CA does not have subscriber or relying party agreements, as all Subscribers and Relying Parties are internal to Apple.

2.5. Financial responsibility

This section sets forth policies as requirements on the Software Update Sub-CA related to indemnification by Relying Parties and disclosure of fiduciary relationships in relying party agreements.

2.5.1. Indemnification by Subscribers and Relying Parties

The Software Update Sub-CA does not have subscriber or relying party agreements, as all Subscribers and Relying Parties are internal to Apple.

2.5.2. Fiduciary relationships

The Software Update Sub-CA does not have subscriber or relying party agreements, as all Subscribers and Relying Parties are internal to Apple.

2.6. Interpretation and enforcement

The Software Update Sub-CA does not have subscriber or relying party agreements, as all Subscribers and Relying Parties are internal to Apple.

2.6.1. Governing law

Not applicable.

2.6.2. Severability, survival, merger, notice

Not applicable.

2.6.3. Dispute resolution procedures

Not applicable.

2.7. Fees

This section sets forth policies associated with any fees charged to Subscribers or Relying Parties for CA services.

2.7.1. Certificate issuance or renewal fees

No fees are charged for this service.

2.7.2. Certificate access fees

No fees are charged for this service.

2.7.3. Revocation or status information access fees

No fees are charged for this service.

2.7.4. Fees for other services

No other fees are charged for CA services.

2.7.5. Refund policy

Not Applicable.

2.8. Publication and repository

Apple operates a repository where this CPS, Sub-CA Certificates, and CRLs are published.

2.8.1. Publication of CA information

The repository can be found at https://www.apple.com/certificateauthority.

2.8.2. Frequency of publication

The CPS will be published in the repository after approval by the Apple PA. Sub-CA Certificates and CRLs are published in the repository after issuance.

2.8.3. Access controls

Subscribers and Relying Parties have unrestricted read access to the repository through supported interfaces.

2.9. Compliance audit requirements

The Software Update Sub-CA adopts wholly all policies under this section in the CP.

2.10. Conditions for applicability

This section sets forth practices related to the use of the Software Update Sub-CA.

2.10.1. Permitted uses

Software Update Signing Certificates may be used to digitally sign software packages in order to authenticate the source of the software package as Apple, and validate the integrity of the software package (it is complete and unaltered).

2.10.2. Limitations on use

The Software Update Sub-CA does not allow its Certificates to be used to create a Certification Authority or its private keys to sign a Certificate issued by another Certification Authority.

Except for administrative Certificates (e.g. OCSP Certificates), Certificates issued by the Software Update Sub-CA shall not be used for any purpose that is not identified in this CPS §2.10.1 as a permitted use.

2.11. Obligations

This section defines the obligations of the participants of the PKI.

2.11.1. General Sub-CA obligations

The Software Update Sub-CA will:

- Conform its operations to the CP and to this CPS.
- Issue and publish Certificates in a timely manner in accordance with the CP and this CPS.
- Revoke Certificates upon receipt of a valid request to revoke the Certificate from a person authorized to request such a revocation. The validity of the request and the

authorization of the person making the request will be determined by an Apple internal process.

- Publish Certificate revocation information on a regular basis, in accordance with the CP and this CPS.

2.11.2. Notification of issuance to Subscribers

Since the Subscribers are internal to Apple, notification of issuance to Subscribers is provided via an Apple internal process.

2.11.3. Notification of issuance to others

The Software Update Sub-CA does not provide notification of issuance to parties other than Apple.

2.11.4. Notification of revocation to Subscribers

Since the Subscribers are internal to Apple, notification of revocation to Subscribers is provided via an Apple internal process.

2.11.5. Notification of revocation to others

The Software Update Sub-CA does not provide notification of revocation to parties other than Apple.

2.11.6. Registration Authority obligations

Not applicable, a Registration Authority is not being used.

2.11.7. Subscriber obligations

The Software Update Sub-CA does not have subscriber or relying party agreements, as all Subscribers and Relying Parties are internal to Apple.

2.11.8. Relying Party obligations

The Software Update Sub-CA does not have subscriber or relying party agreements, as all Subscribers and Relying Parties are internal to Apple.

3. Key life cycle management

This section sets forth practices related to the key life cycle management controls of the Software Update Sub-CA.

3.1. Sub-CA key generation

Key generation occurs using a secure cryptographic device meeting the requirements as disclosed in the business practices in CP §3.2.

The key pair is generated on a Hardware Security Module ("HSM") that is compliant to at least FIPS 140-2 Level 3.

The Software Update Sub-CA signing key pairs are at a minimum of 2048-bits, using the RSA algorithm.

3.2. Sub-CA private key protection

3.2.1. Sub-CA private key storage

Each Software Update Sub-CA private key is stored in an HSM that is tamper resistant and validated at a minimum level of FIPS 140-2 Level 3.

3.2.2. Sub-CA private key control

There is a separation of physical and logical access to each Software Update Sub-CA private key, and a minimum of two individuals is required for physical access to the HSM where a private key is stored.

3.2.3. Sub-CA key escrow

Sub-CA private keys are backed up but not escrowed.

3.2.4. Sub-CA key backup

Sub-CA private keys are backed up for recovery purposes. Backups are stored in a secured environment, and a minimum of two individuals are required for logical recovery.

3.2.5. Sub-CA key archival

Sub-CA private keys, expired keys, and revoked Sub-CA public key Certificates shall be archived for a minimum of two (2) years beyond the expiration date.

3.3. Sub-CA public key distribution

Sub-CA public keys are contained in X.509 Certificates and made publicly available via Apple-distributed software containing the Certificate.

3.4. Sub-CA key changeover

Sub-CA keys have an active lifetime of up to fifteen (15) years. Distribution of new Sub-CA public key Certificates will be performed in accordance with §3.3 of this CPS.

3.5. Sub-CA-provided Subscriber key management

Not applicable.

4. Certificate life cycle management

This section sets forth practices related to the Certificate life cycle management controls of the Software Update Sub-CA.

4.1. External RA requirements

An external Registration Authority is not utilized.

4.2. Certificate registration

Certificates are issued at the request of authorized Apple employees in accordance with internally documented business practices.

4.3. Certificate renewal

Certificates are renewed at the request of authorized Apple employees in accordance with internally documented business practices.

4.4. Certificate rekey

Certificates are rekeyed at the request of authorized Apple employees in accordance with internally documented business practices.

4.5. Certificate issuance

Certificates will be issued at the request of authorized Apple employees in accordance with internally documented business practices.

4.6. Certificate acceptance

Certificates shall be deemed accepted and valid immediately after the Subscriber uses them for the first time.

4.7. Certificate distribution

Software Update Signing Certificates are not made available in a public repository. Apple may, at its discretion, include these Certificates in Apple-distributed software.

Sub-CA Certificates are made available at https://www.apple.com/certificateauthority. CRLs are made available at the location indicated in the CRL distribution points extension.

4.8. Certificate revocation

Certificates may be revoked by authorized Apple employees in accordance with internal business practices. Certificates may be revoked at Apple's sole discretion for reasons including, but not limited to actual or suspected private key compromise, or hardware or software failures which render the private key inoperable.

4.9. Certificate suspension

Certificate suspension is not supported.

4.10. Certificate status

The Apple Software Update Sub-CA utilizes two methods for Certificate validation: CRL and OCSP. Refer to the CRL Distribution Point ("CDP") and/or the Authority Information Access ("AIA") extensions in the Certificates for the status information method used and location.

4.10.1. CRL usage

Subscribers and/or Relying Parties may use a CRL, which is updated periodically at Apple's sole discretion, to determine the status of a particular Certificate. Revoked Certificates remain in the CRL until the Certificates have expired. More than one CRL may be valid at a particular time.

4.10.2. OCSP usage

Subscribers and/or Replying Parties may use OCSP to determine the status of a particular Certificate. Revoked Certificates remain marked as "revoked" for the Certificate lifetime. Delegate Certificates signed by an Apple Software Update Sub-CA are used to sign OCSP responses. More than one OCSP responder Certificate can be in operation at the same time.

OCSP 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, which are not digitally signed.

4.10.3. OCSP designated responder Certificates

Details of the Certificate used to sign the OCSP responses are as follows:

- Effective life of the Certificate may vary at Apple's discretion.
- More than one valid OCSP designated responder Certificate may exist at one time.
- Each OCSP designated responder Certificate will have a unique public/private key pair.
- Suspension of the OCSP designated responder Certificates is not supported.

4.11. Certificate profile

4.11.1. Software Update Signing Certificates

Software Update Signing Certificates issued by a Software Update Sub-CA conforms to the X.509 version 3 Certificate format. Each Certificate contains the following fields:

Field	Value
X.509 Version	Version 3
Serial Number	Serial Number unique among other Certificates issued by the Sub-CA.
Signature Algorithm	SHA-1 with RSA Encryption or SHA-256 with RSA Encryption
Issuer DN	Inherited from the Sub-CA
Validity	Certificates are valid for up to ten (10) years.
Subject DN	The Distinguished Name will include the Common Name, Organization, Country, and may include Organizational Unit.
Public Key	2048-bit RSA
Certificate Extensions	
Extension	Value
Authority Key Identifier	Non-critical Contains Subject Key Identifier from Issuing CA
Subject Key Identifier	Non-critical 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey
Key Usage	Critical digitalSignature
Extended Key Usage	Critical 1.2.840.113635.100.4.1 (Apple Code Signing) or

	1.2.840.113635.100.4.1.1 (Apple Code Signing Development)
Certificate Policies	Non-critical Policy ID: 1.2.840.113635.100.5.1 (Apple Certificate Policy) CPS: https://www.apple.com/certificateauthority User Notice Text: Reliance on this certificate by any party assumes acceptance of the then applicable standard terms and conditions of use, certificate policy and certification practice statements.
Basic Constraints	Critical cA=False
CRL Distribution Point	Non-critical Derived from the Issuing CA For example, http://crl.apple.com/softwareupdateca.crl
Authority Information Access	Non-critical The HTTP URI for the OCSP service
Custom Extension	Non-critical Apple Certificates for Code Signing Production Software Updates (1 2 840 113635 100 6 1 29 2) or Apple Certificates for Code Signing Development Software Updates (1 2 840 113635 100 6 1 29 1)

4.12. CRL profile

A CRL issued by a Software Update Sub-CA will conform to the X.509 version 2 CRL format. Each CRL shall contain, at a minimum, the following fields which are utilized by the Software Update Sub-CA:

- Signature Algorithm of SHA-1 with RSA Encryption or SHA-256 with RSA Encryption
- Issuer matching the Software Update Sub-CA Certificate's Distinguished Name
- "This Update" with the time of CRL issuance
- "Next Update" defining the period of validity

- Authority Key Identifier extension
- List of Revoked Certificates

4.13. OCSP designated responder Certificates

A Certificate issued by a Software Update Sub-CA for the purpose of signing OCSP responses shall conform to the X.509 Certificate format and shall contain, at a minimum, the following data elements:

- Serial Number
- Subject Distinguished name
- Issuer Distinguished name
- Validity date range
- Modulus (Size in bits)
- Signature Algorithm

4.14. Integrated circuit cards

Not applicable.

5. Environmental controls

This section sets forth practices related to the environmental controls of the Apple Software Update Sub-CA.

5.1. CPS administration

Apple has designated a management group with final authority and responsibility for specifying and approving the Software Update Sub-CA's CPS.

This authorized body has performed an assessment to evaluate business risks and determine the security requirements and operational procedures to be included in the CPS for the following:

- Key life cycle management controls
- Certificate life cycle management controls
- CA environmental controls

The Software Update Sub-CA makes available its public CPS to all Subscribers and Relying Parties, including any revisions that occur from time to time.

Any changes to the Software Update Sub-CA's CPS, along with the effective date of the changes, shall be reviewed by the PA, and posted in a timely manner.

5.2. CA termination

After a decision to terminate a Software Update Sub-CA operations has been made in accordance with CP §5.2, the Sub-CA will cease to issue new Certificates.

A risk assessment will be performed by the Apple PA to determine the plan of action to terminate the Sub-CA which may include destruction of the private key.

5.3. Confidentiality

The Sub-CA will keep the following information confidential at all times:

- All private signing keys
- Security audits, parameters, and mechanisms
- Personal or non-public information on Sub-CA Subscribers and Relying Parties

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

The following information shall not be considered confidential:

- The Sub-CA and Software Update Signing Certificates
- CRLs issued by the Sub-CA and Certificate revocation reason codes
- OCSP responses
- Information contained in this CPS and the CP

5.4. Intellectual property rights

All public and private keys, Certificates, CRLs, information provided via OCSP, this CPS, and the CP are the property of Apple.

5.5. Physical security

Physical protection is achieved through the creation of clearly defined security perimeters with appropriate physical barriers to entry around the business premises and facilities. Details of the physical security policies and procedures are in appropriate security documents.

Equipment is located or protected to reduce the risks from environmental threats and hazards, including but not limited to power disruption or failure; telecommunications disruption or failure; fire or water exposure; and opportunities for unauthorized access.

5.6. Business continuity management

Apple has business continuity plans to maintain or restore Sub-CA business operations in a timely manner following interruption or failure of critical business processes.

5.7. Event logging

5.7.1. Archiving

The Software Update Sub-CA archives event journal data on a periodic basis.

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

5.7.2. Event journal reviews

Current or archived event journals may only be retrieved by authorized individuals and only for valid business or security reasons.

Event journals are reviewed periodically.

The review of current and archived event journals includes the identification and follow-up of exceptional, unauthorized, or suspicious activity.

6. Revision history

Issue Number	Issue Date	Details
1.0	04/26/05	Initial release.
1.1	05/18/06	Updated all sections with a new numbering scheme and minor formatting changes. Additionally, updated the content in several sections to more specifically reflect business practices. Added revision history section.
1.2	1 0/26/07	Made updates to reflect change in company name.
1.3	04/26/18	Made changes to include OCSP for certificate status checking, update certificate profile, key, and HSM requirements, and clarify business practices.