Apple Inc.
Certification Authority
Certification Practice Statement
Software Update

Version 1.2
Effective Date: October 26, 2007

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"). Where the CP defines policies that all applicable Apple Sub-CA's are required to follow, this CPS provides more detailed information about the practices employed by the Software Update Sub-CA 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 Software Update Sub-CA.

This CPS is intended to inform participants in Apple's Public Key Infrastructure ("PKI"), including entities that have been issued a Certificate by the Software Update Sub-CA and entities that may choose to place reliance on those Certificates. These participants, called Subscribers and Relying Parties, respectively, should consider the practices of the Software Update Sub-CA and practices of the Apple Root CA, as disclosed in the Apple CP, when choosing whether or not to participate in the Apple PKI. If the Subscriber and Relying Party choose to participate in the Apple PKI, they agree to be bound by the terms of the CP, this CPS, and applicable Subscriber and Relying Party agreements.

Apple Inc. ("Apple") established the Apple Root Certification Authority ("Apple Root CA") and the Apple PKI in support of the generation, issuance, distribution, revocation, administration and management of public/private cryptographic keys that are contained in CA-signed X.509 Certificates. The Apple PKI is intended to support internal and external Apple cryptographic requirements, where authentication of an organization or individual presenting a digitally signed or encrypted object to a Relying Party is of benefit to participants in the Apple PKI.

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 document for the table of acronyms used within this document.

1.3. Definitions

For the purposes of this CPS, the term "Subscriber" refers to authorized personnel within the Apple software update team and development teams that avail themselves of the services provided by the Software Update Sub-CA. Refer to the CP for all other definitions used within this document.

2. General business practices

This section establishes and sets forth the general business practice 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 Apple CP document.

2.2. Community and applicability

This CPS is applicable to all Certificates issued by the Software Update Sub-CA. The Software Update Sub-CA issues and administers Certificates where the corresponding private key may be used to digitally sign software such that the certified public key can be used to:

- Authenticate the source of the software is Apple.
- Verify the integrity of the software package (it is complete and unaltered).

2.3. Contact details

The contact information for this CPS is:

Apple CA Policy Authority
C/O General Counsel
Apple Inc.
1 Infinite Loop, Cupertino, CA 95014

1 (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

This section is not applicable because there are no subscriber agreements.

2.4.5. Private key compromise

This section is not applicable because there are no subscriber agreements.

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.

2.7.5. Refund policy

Not Applicable.

2.8. Publication and Repository

The Software Update Sub-CA operates a repository where public Certificates and CRLs along with other public information are published and accessible to Subscribers or Relying Parties.

2.8.1. Publication of CA information

The latest version of this CPS for the Software Update Sub-CA can be found at http://www.apple.com/certificateauthority/

2.8.2. Frequency of publication

All public key Certificates and CRLs issued by the Software Update Sub-CA will be published in the Software Update Sub-CA repository at the time of issuance.

2.8.3. Access controls

All Subscribers and Relying Parties shall have access to the Software Update Sub-CA repository through supported interfaces.

2.9. Compliance audit requirements

This 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

The Software Update Sub-CA will create keys, manage keys, issue Certificates, manage key lifecycles, manage certificate life cycles, operate a repository, and perform other functions to support the distribution of Apple software to end users.

Issued 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 will not allow its Certificates to be used to create a CA or to allow its private key to sign a Certificate issued by another CA.

The Software Update Sub-CA Certificates 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 sets forth policies related to the obligations of the Software Update Sub-CA, Subscribers and Relying Parties.

2.11.1. General Software Update Sub-CA Obligations

The Software Update Sub-CA shall:

- Conform its operations to the Apple Certificate Policy (CP) and to this CPS, as the same may be amended from time to time.
- Issue and publish Certificates in a timely manner in accordance with the Apple Certificate Policy (CP) document and this CPS.
- Revoke Certificates the Software Update Sub-CA issued, 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 a CRL on a regular basis, in accordance with the Apple Certificate Policy (CP) document and this CPS.

2.11.2. Notifications of issuance by Software Update Sub-CA to Subscriber

Notification of issuance of a new Certificate is deemed to have taken place when a software package signed with the new Certificate is released.

2.11.3. Notification of issuance by Software Update Sub-CA to others

No notification of issuance to others will take place.

2.11.4. Notification of revocation by Software Update Sub-CA to Subscriber

Not applicable as there is no subscriber agreement.

2.11.5. Notification of revocation by Software Update Sub-CA to others

No notification of revocation to others will take place.

2.11.6. Registration Authority obligations

Not applicable, a Registration Authority is not being used.

2.11.7. Subscriber obligations to Software Update Sub-CA

Subscribers are all internal to Apple, so subscriber agreements do not exist and this section is not applicable.

2.11.8. Relying Party obligations to Software Update Sub-CA

There will be no relying party agreement and therefore no Relying Party obligations.

2.12. Conditions for use of the Certificate in software updates

Currently, signed software updates are only provided to customer systems via the Mac OS X Software Update client. Only Apple-provided software is made available via the Software Update client.

Conditions to check for when installing a package:

Condition	Result
Software package is not signed and the originator is Apple	Do not install, Notify user
Software package is signed with bad signature	Do not install, Notify user
Software package was signed but Certificate is revoked	Do not install, Notify user
Software package is Signed, but the CRL is inaccessible (system is not on the network, or network failure, or revocation server error).	Install at user option
Software package is signed and verifies correctly	Install update
Software package is signed and verifies correctly, but the	Do not install, Notify user

Certificate contains the Apple Code Signing (Development) Extended Key Usage purpose	

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. Software Update 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 140-1 Level 4.

The Software Update Sub-CA signing key pair is at a minimum of 1024-bits, using the RSA algorithm.

3.2. Software Update Sub-CA private key protection

3.2.1. CA private key storage

Each .Software Update Sub-CA private key is stored in a Hardware Security Module (HSM) that is tamper resistant and certified at a minimum level of FIPS 140-1 Level 4.

3.2.2. 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. CA key escrow

The Software Update Sub-CA private key shall not be placed in escrow.

3.2.4. CA key backup

Software Update Sub-CA private keys are backed up for recovery purposes. Backups are stored in a secured environment, and m of n secret shares are required for logical recovery.

3.2.5. CA key archival

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

3.3. Software Update Sub-CA public key distribution

The Software Update Sub-CA public key will be contained in an X.509 Certificate and made publicly available via Apple-distributed software containing this Certificate.

3.4. Software Update Sub-CA key changeover

The Software Update Sub-CA private signing key shall have an active lifetime of not more than eight (8) years and the corresponding public key Certificate shall have an active lifetime of not more than eight (8) years.

Upon the end of the private key's lifetime, a new Software Update Sub-CA signing key pair shall be generated. All subsequently issued Certificates and CRLs shall be signed with the new private signing key. The corresponding new Software Update Sub-CA public key Certificate will be made publicly available.

3.5. Software Update 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 by the Software Update Sub-CA.

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

Issued Certificates are valid for a minimum of one (1) year, and a maximum of five (5) years, unless revoked.

Certificates issued with the Apple Code Signing purpose in the Extended Key Usage extension are used to sign and verify signatures of production versions of Apple-distributed software.

Certificates issued with the Apple Code Signing (Development) purpose in the Extended Key Usage extension are used to sign and verify signatures of internal, unreleased, development versions of Apple-distributed software.

4.6. Certificate acceptance

Upon issuance, Certificates are stored in a local repository on the Software Update Sub-CA proxy server. Certificates shall be deemed accepted and valid immediately after issuance.

4.7. Certificate distribution

Access to the Software Update Sub-CA proxy server repository is granted to authorized Apple employees in accordance with internally documented business practices. Apple may, at its discretion, include Certificates in Apple-distributed software.

4.8. Certificate revocation

Certificates may be revoked by authorized Apple employees in accordance with internally documented 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.

Revocation events are recorded in a journal that is kept for the lifetime of the Software Update Sub-CA. All revocations are permanent; once a leaf Certificate is revoked, it cannot be returned to operation. The revocation event journal may be retained indefinitely.

4.9. Certificate suspension

Certificate suspension is not supported. Compromised keys result in completely new key sets and Certificates being issued.

4.10. Certificate status

Certificate status is published via a Certificate Revocation List (CRL) which is updated periodically at Apple's sole discretion. The availability and contents of the CRL are used to determine the validity of signatures generated by Software Update Sub-CA leaf Certificates.

Certificates and CRLs issued by the Software Update Sub-CA shall be retained for a period of not less than two (2) years.

4.11. Certificate profile

A Certificate issued by the Software Update Sub-CA shall conform to the X.509 version 3 Certificate format. Each Certificate shall contain the following fields which are utilized by the Software Update Sub-CA:

- Subject Distinguished Name in the form of an X.500 Distinguished Name. The Country, Organization, and Organizational Unit portions of an issued Certificate's Distinguished Name must match those of the Software Update Sub-CA Certificate. The Common Name, or any additional portions, are specified by the authorized Apple employee requesting the Certificate for informational purposes only, and need not be unique.
- Issuer Distinguished Name matching the Software Update Sub-CA Certificate's Distinguished Name.
- Serial Number unique among other Certificates issued by the Software Update Sub-CA.
- Signature Algorithm of SHA-1 with RSA Encryption.
- Start Date and End Date defining the period of validity.
- RSA Public Key.
- Key Usage extension, marked critical, allowing use for Digital Signature.
- Basic Constraints extension, marked critical, disallowing use as a Certificate Authority.
- Extended Key Usage extension, not critical, with a purpose containing either Apple Code Signing (1.2.840.113635.100.4.1) or Apple Code Signing (Development) (1.2.840.113635.100.4.1.1).
- Subject Key Identifier extension, not critical.
- Authority Key Identifier extension, not critical.
- Certificate Policies Extension, not critical, with a Policy ID of Apple Certificate Policy (1.2.840.113635.100.5.1) referring to the CP, and Certification Practice Statement and User Notice qualifiers referring to this CPS.
- CRL Distribution Points extension, not critical.

- Certificate Authority Information Access extension, not critical, with a CA Issuers method.

4.12. CRL profile

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

- Signature Algorithm of SHA-1 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

The CRL can be obtained from:

https://www.apple.com/certificateauthority/swupdate.crl

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

The Software Update Sub-CA keys will be destroyed using the key destruction method supported by the Software Update Sub-CA HSM.

Apple will make arrangements for the long-term storage of sensitive Subscriber records.

5.3. Confidentiality

The Software Update Sub-CA shall keep the following information confidential at all times:

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

Except as required to support the WebTrust audit performed by an independent external audit firm, confidential information should not released to 3rd 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.

The following information shall not be considered confidential:

- Information included in the public Certificates
- Any CRL issued by the Software Update Sub-CA
- The Apple Software Update Sub-CA public Certificate or any leaf Certificates
- Information contained in the CA's CPS and CP documents

- Any certificate revocation reason code

5.4. Intellectual property rights

All public and private keys, Certificates, CRLs, the CPS and 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 Software Update Sub-CA 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

The Software Update Sub-CA has business continuity plans to maintain or restore the Software Update Sub-CA's 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.

The Software Update Sub-CA maintains archived event journals at a secure off-site location for a predetermined period.

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 a validation of the event journals' integrity, and 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	10/26/07	Made updates to reflect change in company name.