Apple Inc.
Certification Authority
Certificate Policy

Version 1.4
Effective Date: July 18, 2012

Table of Contents

1. Introduction 4
1.1. Trademarks 4
1.2. Table of acronyms 4
1.3. Definitions 5
2. General business practices 9
2.1. Identification 9
2.2. Community and applicability 9
2.2.1. Apple Root CA 9
2.3. Contact details 9
2.4. Apportionment of liability 9
2.4.1. Warranties to Subscribers and Relying Parties 10
2.4.2. CA disclaimers of warranties 10
2.4.3. CA limitations of liability 10
2.4.4. Subscriber warranties 10
2.4.5. Private key compromise 11
2.4.6. Subscriber and Relying Party liability 11
2.5. Financial responsibility 11
2.5.1. Indemnification by Subscribers and Relying Parties 11
2.5.2. Fiduciary relationships 11
2.6. Interpretation and enforcement 11
2.6.1. Governing law 11
2.6.2. Severability, survival, merger, notice 11
2.6.3. Dispute resolution procedures 11
2.7. Fees 11
2.7.1. Certificate issuance or renewal fees 12
2.7.2. Certificate access fees 12
2.7.3. Revocation or status information access fees 12
2.7.4. Fees for other services 12
2.7.5. Refund policy 12
2.8. Publication and Repository 12
2.8.1. Publication of CA information 12
2.8.2. Frequency of publication 12
2.8.3. Access controls 12
2.9. Compliance audit requirements 13
2.9.1. Frequency of entity compliance audit 13
2.9.2. Auditor's relationship to audited party 13
2.9.3. Topics covered by the audit 13
2.9.4. Actions taken as a result of deficiency 13
2.9.5. Communications of results 13
2.10. Conditions for applicability 13
2.10.1. Permitted uses 13
2.10.2. Limitations on use 14
2.11. Obligations 14
2.11.1. General CA obligations 14
2.11.2. Notification of issuance by CA to Subscriber 14
2.11.3. Notification of issuance by CA to others 14
2.11.4. Notification of revocation by CA to Subscriber 15
2.11.5. Notification of revocation by CA to others 15
2.11.6. Registration Authority obligations 15

2.11.7. Subscriber obligations to CA 15
2.11.8. Relying Party obligations to CA 15
3. Key life cycle management 17
3.1. CA key pair generation 17
3.2. CA private key protection 17
3.3. CA public key distribution 17
3.4. CA key changeover 17
3.5. Subscriber key pair generation 18
3.6. Subscriber private key protection 18
4. Certificate life cycle management 19
4.1. External RA requirements 19
4.2. Certificate registration 19
4.3. Certificate renewal 19
4.4. Certificate rekey 19
4.5. Certificate issuance 19
4.6. Certificate acceptance 20
4.7. Certificate distribution 20
4.8. Certificate revocation 20
4.9. Certificate suspension 21
4.10. Certificate status 21
4.11. Certificate profile 22
4.12. CRL profile 22
4.13. Integrated circuit cards 23
5. Environmental controls 24
5.1. CP & CPS administration 24
5.2. CA termination 24
5.3. Confidentiality 24
5.4. Intellectual property rights 25
5.5. Physical security 25
5.6. Business continuity management 25
5.7. Event logging 26
6. Revision history 27

1. Introduction

This Apple Certificate Policy ("CP") sets forth the business, legal, and technical requirements governing the use of Apple CA Certificates by participants in the Apple Public Key Infrastructure ("PKI").

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.

This document assumes the reader is familiar with the general concepts of digital signatures, certificates, and PKI. If the reader is new to PKI 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.

1.1. Trademarks

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

1.2. Table of acronyms

The following acronyms are used within this document. These acronyms are defined at CP §1.3.

Acronym	Term
CA	Certification Authority
CAMT	Certification Authority Management Team
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
HSM	Hardware Security Module
MAC	Message Authentication Code
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

1.3. Definitions

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

Term	Definition
Apple Certification Authority	Any or all of (1) the Apple Root CA and/or (2) the Sub-CA's stated at CP §2.2.
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 (containing required check values) for the purpose of obtaining a certificate or requesting the CA to perform an administrative function.
Certification Authority	This is an entity that securely operates a software package that generates public/private key pairs, signs subscriber's public key in a certificate, and stores certificates in a repository. The CA securely operates a software package that stores subscriber public keys in a directory. These keys can be used for generating electronic signatures, encrypting documents so only the intended recipient(s) can read them, and ensuring the documents have not been altered. The CA stores a subscriber's public key in a certificate, which is then digitally signed by the CA as the valid public key. All certificates are stored in a directory managed by the CA. Certificates and keys are generated and managed according to the lifecycles described in this CP and a CPS.
Certification Authority Management Team	The group of people within Apple responsible for defining CA policy and supporting ongoing operations.

Term	Definition
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 an authentication code ("MAC") created and signed by its issuer. These authentication codes 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	This is a corporate policy that sets forth business practices, system integrity controls, and environmental controls associated with all Apple CAs.
Certification Practice Statement	Each CA within the Apple PKI sets forth specific operational practices and procedures associated with each CA's business practices, integrity controls, and environmental controls.
Certificate Revocation List	This is a digitally signed list of certificates that are no longer valid because the accompanying private key has been lost, stolen, or compromised, or the CA has revoked the certificate. As an example: A relying party may check to see if a certificate that they receive is listed on a CA's revocation list. If the Certificate is listed, the relying party knows that any signature or source of an encrypted object should not be trusted as of the date the CA added the certificate to the CRL.
Directory	A system operated and administered by a CA that supports the storage and retrieval of X.509 certificates and CRLs managed by the CA. This system may support X.500 Directory Services, or implement similar technology. Whatever service is used, it should support the X.520 naming convention (distinguished names) to uniquely identify every subscriber to whom a certificate is issued by a CA. This may also be referred to as a repository.
Distinguished Name	Within the scope of a CA related to the issuance and management of certificates, this is a value that uniquely identifies each subscriber to whom a certificate is issued. The value conforms to the X.520 standard. An example: The first subscriber has a certificate issued where the distinguished name is "Jane Doe". A second subscriber requests Jane Doe as well, but must provide a suffix that makes the resulting distinguished name unique. This could be "Jane Doe 23".

Term	Definition
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 140-1 level 4) device. Key access must be authenticated and recorded in audit logs.
Message Authentication Code	This is a value used to certify and verify the integrity of a document or file. The value is calculated using a one-way hash algorithm, like SHA-1, as a digest of the document or file that is then digitally signed using a private key and the Digital Signature Algorithm ("DSA").
Message Digest	As used herein, this is the same as a message authentication code.
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 person or business entity that receives an X.509 certificate (issued to a subscriber by a CA) and has a vested interest of some kind in the validity of the certificate and any attributes or encrypted objects created using the subscriber's private key, corresponding to the public key contained in the certificate.
Repository	As used, same as Directory.
Root Certification Authority	This is a CA that is at the top of a hierarchical PKI network.
Split-Knowledge Technique	A security procedure where no single individual possesses the equipment, knowledge or expertise to view, alter or otherwise have access to sensitive or confidential information in a particular PKI.

Term	Definition
Subscriber	This is a person or business entity that establishes a relationship with a CA for the purpose of obtaining a private encryption key and certificate containing the corresponding public key.
Subscriber Agreement	An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates. An Apple CA may choose to include a subscriber agreement as part of an End User License Agreement (EULA). If the subscriber agreement is contained in the EULA, a Subscriber is considered to have accepted the subscriber agreement when the Subscriber accepts the terms and conditions of the EULA and/or upon receipt of a Certificate issued to the Subscriber by an Apple CA.
Subordinate Certification Authority	This is a CA that is a node of the Root CA within a hierarchical PKI network. The scope and services delivered by this Sub-CA are specified in its CPS.

2. General business practices

2.1. Identification

For the purposes of this CP, 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 Sub-CAs, 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.

For the purposes of this CP, the term "Apple CA" refers to any or all of the Apple Root CA and/or the Sub-CA's stated at CP §2.2. Details of policies and procedures that are unique to these Sub-CAs shall be documented in each Sub-CA's respective Certification Practice Statement ("CPS").

In addition to the CAs described at CP §2.2, the Apple PKI may establish additional root certificates and subordinate certification authorities that are outside the scope of this CP. The Apple PKI may actively use and decommission these Certificates and certification authorities for the purpose of generating and using cryptographic keys, and issuing, distributing, revoking, administering, and managing digital Certificates. Actions taken by the Apple Root CA or other Apple root certificates with respect to these subordinate certification authorities, and the actions of these subordinate certification authorities themselves, will occur without public notice or consent, or inclusion in this or any other publicly available policy.

2.2. Community and applicability

2.2.1. Apple Root CA

The Apple Root CA administers the signing, issuance, and revocation of Certificates used to establish and authenticate an Apple Sub-CA. The Root CA, or a delegated leaf of the Root CA, is also used for signing the CA's Certificate Revocation Lists ("CRL"). Each Sub-CA CPS shall describe the types of and uses of the certificate services provided.

2.3. Contact details

The contact information for this CP is:

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

(408) 996-1010
policy_authority@apple.com

2.4. Apportionment of liability

Any warranties, disclaimers of warranty, and limitations of liability are set forth by either subscriber, relying party, end user license agreements or terms and conditions accompanying a Certificate.

An Apple Sub-CA shall describe in the respective CPS its use of subscriber, relying party and/or end user license agreements. Further, if applicable, the CPS must state how subscriber and/or relying party agreements are communicated to and accepted by Subscribers and/or Relying parties.

2.4.1. Warranties to Subscribers and Relying Parties

The granting of warranties to Subscribers and Relying parties is at the sole discretion of the Sub-CA, subject to the limitations set forth herein. Where warranties are granted, they are defined in the Sub-CA's respective subscriber and relying party agreements.

Subscriber agreements used by the Sub-CA may not include any warranty other than the following:

- There are no material misrepresentations of fact in the Certificate known to the entities approving the certificate application or issuing said Certificate
- The entities approving the certificate application or issuing the Certificate have exercised reasonable care in managing the certificate application or creating the Certificate. Apple does not warrant that the process is error free
- Certificates meet all material requirements of the CPS from the applicable Sub-CA
- Revocation services and use of a repository conform to this CP or CPS for the applicable Apple CA

Relying party agreements used by the Sub-CA may not include any warranty other than the following:

- Where a Certificate appears in the repository, that Certificate has been issued to an individual or organization named in the Certificate that represented themselves to Apple as that individual or organization.
- The entities approving the certificate application and issuing the Certificate have substantially complied with the applicable CPS when issuing the Certificate.

2.4.2. CA disclaimers of warranties

Certificates issued by an Apple CA shall not be used to support the trustworthiness, assurance, identity, confidentiality, or nonrepudiation of any monetary transaction.

Except as otherwise permitted within this CP and to the extent permitted by applicable law, subscriber agreements and relying party agreements shall disclaim liability on the part of Apple for all possible warranties, including any warranty of merchantability or fitness for a particular purpose or non-infringement.

2.4.3. CA limitations of liability

To the extent permitted by applicable law, subscriber agreements and relying party agreements shall limit liability on the part of Apple. Limitations of liability shall exclude indirect, special, incidental, and consequential damages.

2.4.4. Subscriber warranties

As stated at CP §2.11.7, Subscriber warranties are handled as obligations on the Subscriber within subscriber agreements or terms and conditions.

2.4.5. Private key compromise

Subscriber agreements shall state that Subscribers are solely responsible for preventing any unauthorized user from having access to any Certificate or private key stored on their computer.

2.4.6. Subscriber and Relying Party liability

Subscribers and Relying parties will hold Apple harmless from any and all liabilities, losses, actions, damages, or claims (including all reasonable expenses, costs, and attorneys fees) arising out of or relating to their use of, or reliance on, any digital Certificate.

2.5. Financial responsibility

This section sets forth policies as requirements on Apple CAs related to indemnification by Relying parties and disclosure of fiduciary relationships in subscriber and/or relying party agreements.

2.5.1. Indemnification by Subscribers and Relying Parties

As set forth in the policies and practice statements, any subscriber and/or relying party agreement may include an indemnification clause requiring Subscribers and/or Relying parties to indemnify Apple.

2.5.2. Fiduciary relationships

If applicable, the fiduciary relationship between Apple and agents, fiduciaries, trustees, or other representatives of Subscribers or Relying parties shall be set forth in subscriber and/or relying party agreements established by any Apple CA.

2.6. Interpretation and enforcement

This section sets forth policies as requirements on the Apple Sub-CAs related to interpretation and enforcement provisions for applicable agreements.

2.6.1. Governing law

Governing law will be stated in the subscriber agreements and relying party agreements or applicable end user license agreements.

2.6.2. Severability, survival, merger, notice

The use of these clauses is disclosed in the relevant CPS.

2.6.3. Dispute resolution procedures

Dispute resolution procedures will be set forth in the respective CPS.

2.7. Fees

This section sets forth policies associated with any fees charged to Subscribers or Relying parties for certification authority services.

All detailed policies and procedures for publication or notification to Subscribers by an Apple CA related to any service fee shall be documented in the Apple CA's CPS.

2.7.1. Certificate issuance or renewal fees

The Apple Root-CA public Certificate will be distributed without a fee being charged.

Apple Sub-CAs may charge fees for CA services to Subscribers depending on the business unit administering the Sub-CA. Specific fees for CA services will be established and published to Subscribers as a part of the normal course of business.

2.7.2. Certificate access fees

The Root-CA public Certificate shall be freely published and distributed.

An Apple Sub-CA may charge fees to Subscribers for certificate access services that could include certificate management, storage and distribution.

2.7.3. Revocation or status information access fees

An Apple CA operating a repository shall not charge fees to Subscribers or Relying Parties related to certificate status requests received and processed.

2.7.4. Fees for other services

Any Apple CA may charge fees to Subscribers or other parties for services performed by the Apple Sub-CA.

2.7.5. Refund policy

If applicable, the Apple Sub-CA shall establish a refund policy as described in the relevant CPS.

2.8. Publication and Repository

The Apple CA may operate a repository where public Certificates and CRLs along with other public information are published and accessible to Subscribers or Relying parties. If applicable, detailed information about specific interfaces supported by the repository will be described in the CPS for the Apple CA.

As referenced in this section, the Apple CA refers to any combination of entities including Root-CA and Sub-CAs.

2.8.1. Publication of CA information

The latest CP is available on the Apple web site at www.apple.com. The CPS for each Apple Sub-CA can be found at http://www.apple.com/certificateauthority/.

2.8.2. Frequency of publication

Public key Certificates and CRLs issued by the Apple CA or Apple sub-CAs will be stored in the Apple CA repository within 24 hours of issuance.

Depending on the Sub-CA and supported applications, public key Certificates and CRLs may be published or distributed through other mechanisms, which may include software patch distributions, electronic mail, or publication on an HTTP server.

2.8.3. Access controls

All Subscribers and Relying parties shall have access to the Apple CA repository through supported interfaces and using authorized accounts.

2.9. Compliance audit requirements

This section sets forth policies related to the audit of the Apple CA policies as documented in this CP.

2.9.1. Frequency of entity compliance audit

An annual audit will be performed by an independent external auditor to assess the adequacy of the Apple CA business practices disclosure and the effectiveness of the CA's controls according to AICPA/CICA WebTrust for Certification Authorities principles and criteria.

2.9.2. Auditor's relationship to audited party

The auditors performing an annual audit shall be from an independent audit firm that is approved to audit according to AICPA/CICA WebTrust for Certification Authorities principles and criteria. Apple will retain the external audit firm, and individual auditors shall not be employees or related to employees of Apple.

2.9.3. Topics covered by the audit

Apple will conduct internal audits periodically during the year and one annual audit to be conducted by an external and independent third party. Topics covered by the annual audit shall include:

- CA Business practice disclosures
- Service Integrity (including key and certificate life cycle management controls)
- CA environmental controls

An Apple CA may perform a self-assessment as needed or at the direction of the Apple CA Policy Authority.

2.9.4. Actions taken as a result of deficiency

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

2.9.5. Communications of results

Audit and assessment results shall be communicated to the PA and may be communicated to the Apple CA Steering Committee, members of the Apple Executive Team, and others as deemed appropriate by the PA.

2.10. Conditions for applicability

This section sets forth policies related to the use of the Apple CA.

2.10.1. Permitted uses

The Root CA shall be permitted to issue, manage, and revoke Certificates that enable the creation, operation, or discontinuation of Sub-CAs. Additionally, the Root CA shall be permitted to create, manage, and destroy cryptographic keys as they relate to the issuance, management, and revocation of delegated leaf Certificates employed to sign CRLs and/or definitive OCSP responses.

Each Sub-CA may create, manage, and destroy cryptographic keys; issue, manage, and revoke Subscriber Certificates; operate a repository; or perform other functions on behalf of its Subscribers and Relying Parties as described in its applicable CPS.

2.10.2. Limitations on use

Certificates issued by the Root CA shall not be used for any purpose other than those explicitly permitted in CP § 2.10.1.

Certificates issued to a Sub-CA by the Root CA shall not be used for any purpose other than those explicitly permitted in CP § 2.10.1. Each Sub-CA shall not allow Certificates it issues to enable the creation of a subordinate certification authority or allow the Sub-CA's private key to sign a Certificate issued by another Certification Authority.

Certificates issued by a Sub-CA shall not be used for any purpose other than those explicitly permitted in the applicable CPS.

2.11. Obligations

This section sets forth policies related to the obligations of Apple CA, Subscribers and Relying parties.

2.11.1. General CA obligations

The Apple Root CA shall:

- Conform its operations to this CP including any amendments thereto.
- Revoke Certificates and publish the related CRL in a timely manner, in accordance with this CP including any amendments thereto.

Each Apple Sub-CA shall:

- Conform its operations to this CP, as amended, and to its CPS.
- Issue and publish Certificates in a timely manner in accordance with this CP and its CPS.
- Revoke Certificates, issued by the Sub-CA, in a timely manner consistent with this CP and its CPS.
- Publish CRLs on a regular and timely basis, or provide OCSP services.

2.11.2. Notification of issuance by CA to Subscriber

Upon issuance of a Subscriber's Certificate, the Apple CA shall notify the Subscriber. The nature of the notification will be commensurate with the intended purpose of the issued Certificate. Apple CAs may employ transparent mechanisms involving minimal user interaction and indirect notification of Certificate issuance. Subscribers should refer to the applicable CPS for details about the notification mechanism(s) employed for a given Certificate.

2.11.3. Notification of issuance by CA to others

In the case where an Apple CA provides notification of issuance to parties other than the Subscriber, the CA shall document the mechanism and nature of the notification in its CPS.

Propagation of the public Apple Root Certificate by Apple or others shall not be considered subject to this policy.

2.11.4. Notification of revocation by CA to Subscriber

Upon revocation of a Subscriber's Certificate, the Apple CA shall notify the Subscriber. The nature of the notification will be commensurate with the intended purpose of the issued Certificate. Apple CA's may employ transparent mechanisms involving minimal user interaction and indirect notification of Certificate revocation. Subscribers should refer to the applicable CPS for details about the revocation notification mechanism(s) employed for a given Certificate.

2.11.5. Notification of revocation by CA to others

In the case where an Apple CA provides notification of certificate revocation to parties other than the Subscriber, the Apple CA shall document the mechanism and nature of the notification in its CPS.

2.11.6. Registration Authority obligations

An RA may initiate or process revocation requests for end-user Certificates, and approve applications for renewing or rekeying Certificates. An Apple CA is not precluded from performing the functions of an RA, nor precluded from employing an authorized third party to perform RA functions. Unless otherwise stated in the applicable CPS, the Sub-CA will perform the functions of the RA for Certificates it issues. Such functions shall be documented in the applicable CPS.

2.11.7. Subscriber obligations to CA

Pursuant to the terms of a Subscriber Agreement with an Apple CA, at a minimum, Subscribers shall be required to:

- Accept all terms and conditions as stated in the Subscriber Agreement (for end-user Subscribers only).
- Provide information that is accurate and complete, in cases where the Subscriber is required to provide information to the Apple CA to obtain the Certificate. The Subscriber will also promptly notify the Apple CA of any changes to this information.
- Be bound by the limitations of liability (for end-user Subscribers only).
- Safeguard their private key from compromise.
- Use Certificates exclusively for legal purposes and in accordance with this CP and the applicable CPS.
- Promptly request that the Apple CA revoke a Certificate if the Subscriber has reason to believe the Certificate's corresponding private key has been compromised.

2.11.8. Relying Party obligations to CA

When an Apple CA has a Relying Party agreement, at a minimum Relying parties shall be required to:

- Accept all terms of the Relying Party agreement as a condition of using or otherwise relying on Certificates, and agree to be bound by the limitations of liability and disclaimers of warranties.
- Restrict reliance on Certificates issued by the Apple CA to the purposes for which those Certificates were issued, in accordance with this CP and applicable CPS.

- Independently assess the appropriateness of the use of a Certificate. Apple shall not be responsible for assessing the appropriateness of the use of a Certificate.
- Not use Certificates beyond the limitations as described in this CP or for purposes prohibited in this CP.

3. Key life cycle management

This section sets forth the business practices associated with Apple CA key life cycle management controls.

3.1. CA key pair generation

The Apple Root CA and Sub-CA signing keys are at least 2048 bits in length, and employ the RSA cryptographic algorithm. The HSM used for key generation and Certificate signing is minimally compliant with FIPS 140-1 Level 4. An Apple CA's signing key will be used to digitally sign Certificates, and may be used to sign CRLs or definitive OCSP responses.

The maximum lifetime of a Root CA Certificate signing key will be thirty (30) years. The maximum lifetime of a Sub-CA Certificate signing key will be fifteen (15) years.

CRL and OCSP response signing keys, if different than the Certificate signing key, are not required to be generated or stored on hardware certified to be FIPS 140-1 compliant. If employed, the maximum lifetime of these CRL or OCSP response signing keys will be one (1) year.

3.2. CA private key protection

The HSM for generating and storing an Apple CA private key shall be minimally certified to FIPS 140-1 Level 4.

There shall be a separation of physical and logical access to an Apple CA's private key to this extent:

- A minimum of two individuals is required for physical access to the hardware module.
- If an Apple CA's private key requires restoration, a Split-Knowledge Technique encompassing individuals, passphrases, and *m* of *n* removable media is required for logical reconstruction.
- Escrow of an Apple CA private key by an external third party is not permitted.
- Apple CA private signing keys, expired keys, and corresponding Certificates shall be archived for a minimum of two (2) years beyond expiration date.
- Apple CAs are not obligated to retain any expired or revoked end-user Subscriber Certificates. Sub-CA's may, at their sole discretion, retain expired or revoked Certificates for a period of time after expiry or revocation, and such practices, if performed, will be documented in the Sub-CA's applicable CPS.

3.3. CA public key distribution

The Apple Root CA's public key shall be contained in a self-signed, X.509 v3 Certificate. This Certificate is distributed in Apple's Mac OS X version 10.4 and higher operating systems, and may be distributed via software update packages provided by Apple, and/or may be made available via the Internet for on-demand distribution to Subscribers and Relying Parties.

Apple Sub-CA public keys shall be contained in X.509 v3 Certificates signed by the Apple Root CA. Sub-CA Certificates may be distributed in Apple's Mac OS X version 10.4 and higher operating systems, software update packages provided by Apple, and/or may be made available via the Internet for on-demand distribution to Subscribers and Relying Parties.

3.4. CA key changeover

Distribution of new public keys due to rekeying the Root CA or Sub-CA Certificates will be performed in accordance with CP §3.3.

3.5. Subscriber key pair generation

If a Sub-CA provides subscriber key pair generation services, details of the Subscriber key pair generation services and the secure distribution mechanism shall be described in the applicable CPS.

If the Sub-CA does not provide subscriber key pair generation services, a Subscriber's cryptographic key pair shall be generated in software on the Subscriber's computer system. The Subscriber's computer system is not required to be FIPS 140-1 certified.

Subscriber key pairs shall be at least 1024 bits in length, and employ the RSA cryptographic algorithm.

The use of cryptographic keys by Subscribers is limited exclusively to the authorized uses stated in this CP and the applicable CPS.

3.6. Subscriber private key protection

An Apple CA may, at its discretion, provide private key backup, archival, and/or escrow services as defined in the applicable CPS. Unless stated otherwise in the applicable CPS, Subscribers should not rely on an Apple CA's backup or archive of the Subscriber's private key. Additionally, Subscriber private keys, if backed-up or archived by an Apple CA, may be destroyed at any time, without notice to the Subscriber and without the Subscriber's consent.

4. Certificate life cycle management

This section sets forth policies related to the management of the certificate life cycle by Apple CAs.

4.1. External RA requirements

In the event an Apple CA uses an external RA, the applicable CPS will outline requirements for interoperation with the RA.

4.2. Certificate registration

Each CA will establish a single naming hierarchy utilizing the Distinguished Names form. All subjects in the Apple PKI shall be unambiguously identified in the naming hierarchy. The requirements for Subscriber application shall be stated in the applicable CPS.

Unless otherwise stated in an applicable CPS, Certificates issued by an Apple CA offer no assurance as to the identity of an individual bearing a Certificate signed by an Apple CA. If an Apple CA issues Certificates authorized to bear more than a minimal level of identity assurance, the procedures performed by the CA to validate the identity of the Certificate applicant upon issuing, rekeying, renewing, or updating a Certificate shall be stated in the applicable CPS.

4.3. Certificate renewal

To the extent necessary, a Subscriber's need to renew a Certificate shall be stated in the applicable CPS.

The Apple CA, upon receiving a request for renewal of a Certificate, shall follow the same process used for the issuance of a new Certificate. However, after submitting necessary identification credentials in connection with the issuance of the original (new) Certificate, a Subscriber may be required to provide only the information that has changed since the prior certificate application for renewal of the Certificate.

Validation of check values or other Subscriber information by the Apple CA will be performed in accordance with CP §4.2

4.4. Certificate rekey

The Apple CA, upon receiving a request for rekey of an end-user Subscriber Certificate, including routine rekey requests and requests for rekey after revocation or expiration, shall follow the same process used for the issuance of a new Certificate.

Validation of check values or other Subscriber information by the Apple CA will be performed in accordance with CP §4.2.

4.5. Certificate issuance

The Apple CA shall issue Certificates to the Subscriber upon successful processing of the Subscriber's Certificate Application. The process of issuance will be complete upon acceptance of the Certificates by the Subscriber.

Refer to CP §2.11.2 for the requirements of an Apple CA to notify Subscribers about issuance of a Certificate. Refer to CP §4.11 for Certificate format, profile requirements, and required extension fields.

4.6. Certificate acceptance

The actions required by the Subscriber to accept a Certificate will be commensurate with the intended purpose of the Certificate. Apple CAs may employ transparent mechanisms involving minimal user interaction and implicit acceptance by the Subscriber of the Certificate. Subscribers should refer to the applicable CPS for specific acceptance requirements.

4.7. Certificate distribution

Each Apple CA shall establish a mechanism for making Certificates and Certificate status checking services available to Subscribers and authorized Relying Parties. Refer to the applicable CPS for details about the established mechanism.

4.8. Certificate revocation

A Sub-CA Certificate may be revoked if any of the following events or circumstances occur:

- The Sub-CA's or Root-CA's management team has reason to believe it's private key has been compromised.
- The Root CA's management team has reason to believe the Sub-CA is violating the terms and conditions.
- The Sub-CA's or Root-CA's management team has reason to believe the Sub-CA's Certificate was issued in a manner materially non-compliant with this Certificate Policy.
- The Sub-CA's or Root-CA's management team has reason to believe the Sub-CA's practices are materially non-compliant with the Sub-CA's CPS and such non-compliant practices will not be remedied or mitigated within a reasonably short period, generally not to exceed six months, and the Apple Root CA Policy Approval Board believes continued use of that Certificate is harmful to the Apple CA.
- The Root CA Certificate that signed the Sub-CA's Certificate is set to expire before the Sub-CA's Certificate, causing potential customer satisfaction, platform interoperability, and PKI service availability issues.
- The Sub-CA requests revocation of its Certificate.

An end-user Subscriber Certificate may be revoked if any of the following events or circumstances occur:

- The Subscriber, or other entity with an expressed or implied responsibility for safeguarding the Subscriber's private key, has reason to believe the Subscriber's private key has been compromised.
- The Sub-CA has reason to believe that the Subscriber's private key has been be compromised.
- The Subscriber has materially breached an obligation, representation, or warranty under the applicable Subscriber agreement if any.
- The subscriber agreement with the Subscriber has been terminated.
- The Subscriber, or other entity that agreed to the terms of the subscriber agreement or EULA under which the Certificate was issued, or the Sub-CA or Root-CA discovers or has reason to believe either (1) the Certificate was issued in a manner not materially in accordance with the procedures required by this CP or applicable CPS, (2) the certificate application is misleading, falsified, or not materially accurate throughout the lifetime of the

Certificate, (3) a material prerequisite to certificate issuance was neither satisfied nor expressly waived by the Sub-CA, (4) the Certificate was issued to a person other than the one named as the subject of the Certificate, or the Certificate was issued without the authorization of the person named as the subject of such Certificate.

- The Subscriber requests revocation in accordance with the applicable CPS.
- The Sub-CA's Certificate that signed the Subscriber's Certificate is set to expire before the Subscriber's Certificate, causing potential customer satisfaction, platform interoperability, and PKI service availability issues.
- The Sub-CA management team, Root-CA management team, or the Apple Policy Authority deems continued use of the Certificate harmful to the Apple CA.

The Root-CA's revocation process supports the secure and authenticated revocation of one or more Certificates and provides a means of communication of such revocation through publication of a CRL updated within 24 hours of authorization of revocation. In addition, revoked Certificates are removed from the CRL after the Certificate has expired.

Each Sub-CA provides a revocation mechanism that provides a means of rapid communication of revoked Certificates. Acceptable Sub-CA revocation mechanisms are described in CP §4.10.

Notification, if any, to an end-user Subscriber that a Certificate has been revoked is defined in the applicable CPS.

4.9. Certificate suspension

The Apple Root-CA and Sub-CAs do not support certificate suspension.

4.10. Certificate status

The Apple Root CA shall issue a CRL at least every 135 days, and not more than 24 hours after it has been determined that revocation of a Certificate is required. See CP §4.8 for circumstances under which a Certificate shall be revoked.

Sub-CAs shall make available revocation information either through a CRL or OCSP, or both. The mechanism shall accurately reflect the status of a given Certificate. CRLs are updated before the expiration of the current CRL. See CP §4.8 for circumstances under which a Certificate shall be revoked.

All Relying parties are solely responsible for their reliance on an Apple Certificate and should check the certificate status of the Subscriber's Certificate using the supported revocation mechanism defined in the Sub-CA's CPS, and the Sub-CA's certificate status using the Root-CA's CRL.

All Apple CAs shall retain all CRLs issued by the CA for a period of not less than two (2) years. Apple CAs are not obligated to retain any expired or revoked Certificates. Sub-CA's may, in their sole discretion, retain expired or revoked Certificates for a period of time after expiry or revocation, and such practices, if performed, will be documented in the Sub-CA's applicable CPS.

Sub-CA's that support OCSP shall disclose in their CPS the content requirements for OCSP requests and the content supplied in definitive OCSP response messages.

All definitive response messages shall be digitally signed either directly by the CA's private key, or with a key belonging to the CA that issued the Certificate(s) in question. Error messages returned by the CA are not digitally signed.

4.11. Certificate profile

A Certificate issued by an Apple CA shall conform to the X.509 Certificate format. The following fields defined by X.509 shall be utilized:

• Version—Set to v3

• Serial Number—Unique values for each Certificate in the CA domain

• Signature algorithm—SHA-1 with RSA Encryption, or stronger

• Issuer—Issuer's distinguished name

• Validity (not valid before and not valid after)• Subject—Certificate subject's distinguished name

• Public Key Information, Algorithm—RSA Encryption

• Public Key Information, Public Key

• Public Key Information, Key Size—1024 bits or greater

• Extension, Key Usage—Marked critical

• Extension, Basic Constraints, CA—Set to "NO" (applicable to Sub-CA's only)

• Extension, Subject Key Identifier

• Extension, Authority Key Identifier

• Extension, Certificate Policies

4.12. CRL profile

If CRL is supported by an Apple CA, the CRL shall conform to the X.509 version 2 CRL format and shall contain, at minimum, the following data elements:

• Version—v2

• Signature—"sha-1withRSAEncryption"

• Last Update—UTC Time

• Next Update—UTC Time

• Revoked Certificates—Listing of information for revoked Certificates.

Certificates issued by an Apple Sub-CA shall specify either the "CRL Distribution Points" extension and/or the "Online Certificate Status Protocol" method of the "Certification Authority Information Access" extension. Apple CA's that support CRLs, including the Apple Root CA, shall specify the "CRL Distribution Points" extension, with the criticality flag set to "NO" and the URI parameter set to the HTTP or HTTPS path of the appropriate CRL.

If OCSP is supported by the Sub-CA, the "Certification Authority Information Access" extension will include at least one "Online Certificate Status Protocol" method and related URI. Specific information about supported OCSP mechanisms, including criticality of the Certification Authority Information Access extension, is stated in the applicable CPS.

A Sub-CA may additionally or alternatively support OCSP. Specific information about a Sub-CA's revocation mechanisms and supported communication protocols is stated in the applicable CPS.

4.13. Integrated circuit cards

The Apple CA does not issue smart cards to Subscribers. Use of integrated circuit cards to store an end-user Subscriber's public or private keys, or end-user Subscriber Certificates, is neither supported nor authorized by the Apple CA.

5. Environmental controls

This section covers disclosure of the operating environment, including security protection and environmental controls.

5.1. CP & CPS administration

Modifications and amendments to this CP shall undergo review and approval by the Apple CA Policy Authority ("PA"). Amended versions shall be posted in a timely manner after being approved by the PA. Any changes to an Apple CA's CPS shall also be posted in a timely manner after being approved by the PA.

Some revisions to this CP may be deemed by the PA to have minimal or no impact on Subscribers and Relying Parties using Certificates and CRLs issued by an Apple CA. Such revisions may be made without notice. In the event that such revisions are deemed by the PA to materially affect current Subscribers or Relying Parties using Certificates and CRLs issued by an Apple CA, the PA will provide notification of the pending changes. Notification will be in the form of an updated CP, posted at http://www.apple.com/certificateauthority/updates for thirty days prior to the effective date of the updated CP.

5.2. CA termination

The Apple Root CA can only be terminated by the Apple CA Steering Committee. In the event the CA is terminated, all Certificates issued by the CA will be revoked and the CA will cease to issue Certificates. The Root CA will provide a minimum of 45 days notice to all business units to which Sub-CA Certificates that have not expired or been revoked. Upon termination, the records of the CA will be archived and retained for a period of three (3) years.

A Sub-CA can be terminated for any of the reasons stated at CP §4.8. Upon termination of a Sub-CA, all Certificates issued by the Sub-CA will be revoked, and the Sub-CA's Certificate will be published on the Root CA's CRL. The records of the CA will be archived and retained for a period of at least two years.

5.3. Confidentiality

This section sets forth policies related to the confidentiality of information maintained or administered by the Apple CA.

The Apple Root CA shall keep the following information confidential, within Apple and its subsidiaries, at all times:

- The Root CA's private keys.
- Information specific to the operation, control, and security of the Root CA.
- Details of annual assessments, advisory engagements, and audits.
- Apple Confidential or non-public information about Sub-CAs.
- Personal or non-public information about Relying Parties.
- Detailed physical and logical security mechanisms.

Apple Sub-CA's shall keep the following information confidential, within Apple and its subsidiaries, at all times:

- The Sub-CA's private keys.

- Subscribers' private keys, if applicable.
- Subscribers' passwords to authenticate to Sub-CA systems, if applicable.
- Personal or non-public information about Subscribers and Relying Parties.
- Detailed physical and logical security mechanisms.

All Apple CA's will comply with requirements to release information, including confidential information, to support the WebTrust audit performed by an independent external audit firm and to law enforcement officials or other entities where required by law or by a court with jurisdiction over the CA.

At the sole discretion of the applicable Root CA or Sub CA management teams, confidential information may be released to third parties if requested by the owner of that information and the identity of the owner can be satisfactorily determined.

The following information is considered non-confidential:

- Information included within any Certificates or CRLs, including revocation reason codes, published by an Apple CA.
- Information contained within this Certificate policy and related Certificate Practice Statements.

5.4. Intellectual property rights

All private keys, Certificates, CRLs, information provided by OCSP (if applicable), this CP, and related certificate practice statements are property of Apple.

5.5. Physical security

Critical Apple CA operations take place within a secure facility to which access is limited to authorized personnel. Cryptographic hardware is physically segregated from the organization's other systems. Access to such systems is controlled by multiple layers of physical security controls, providing reasonable assurance that access is only granted to individuals who require such access to fulfill their job responsibilities.

Details of physical security controls are documented in internal Apple security policies. These policies are not publicly disclosed, but are included within the scope of WebTrust for Certification Authorities. These policies document controls related to the following:

- Physical access controls.
- Environmental controls.
- Backup, business continuity, and disaster recovery controls.

5.6. Business continuity management

Apple has disaster recovery and business continuity plans to address reasonably possible events that can compromise the operation of a critical business function related to the CA. These plans are tested at least annually and the results of the tests are reported to the PA. A recovery site is located at least 50 miles from the primary site and backups of essential business information are performed daily.

Backups of the Root CA and Sub-CA private keys are performed when the key is generated. Backup of private keys follows an m of n backup scheme and taken to secure off-site locations in a timely manner.

5.7. Event logging

Audit trails are backed up in a secure manner on at least a weekly basis. Audit logs are reviewed at least monthly. Unusual events, to the extent any such events are identified and deemed such by the security engineer who reviews the event logs, are summarized and reviewed by the PA and/or Root CA or Sub-CA management team(s) on a quarterly basis.

6. Revision history

Issue Number	Issue Date	Details
1.0	04/26/05	Initial release.
1.1	05/18/06	Updated all sections of the CP 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 addition of new Shared Computers Certificate type and change in company name.
1.3	2/28/12	Updates to reflect use of CP for additional Sub-CAs.
1.4	7/18/12	Minor updates to the key lifecycle management section.