Apple Inc.
Certificate Policy and Certification Practice Statement Apple Corporate Email Certificates

Version 2.3
Effective Date: June 5, 2019

Table of Contents

1. Introduction 5
1.1. Trademarks 5
1.2. Table of acronyms 5
1.3. Definitions 6
2. General business practices 9
2.1. Identification 9
2.2. Community and applicability 9
2.3. Contact details 10
2.4. Apportionment of liability 10
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. Relying Party liability 11
2.5. Financial responsibility 11
2.5.1. Indemnification by Subscribers 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 12
2.9.1. Frequency of entity compliance audit 12
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. Communication 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 Sub-CA obligations 14
2.11.2. Notification of issuance to Subscribers 14
2.11.3. Notification of issuance to others 14
2.11.4. Notification of revocation to Subscribers 15
2.11.5. Notification of revocation to others 15
2.11.6. Registration Authority obligations 15
2.11.7. Subscriber obligations 15
2.11.8. Relying Party 15
3. Key life cycle management 16
3.1. Sub-CA key generation 16
3.2. Sub-CA private key protection 16
3.2.1. Sub-CA private key storage 16
3.2.2. Sub-CA private key control 16
3.2.3. Sub-CA key escrow 16
3.2.4. Sub-CA key backup 16
3.2.5. Sub-CA key archival 16
3.3. Sub-CA public key distribution 16
3.4. Sub-CA key changeover 17
3.5. Sub-CA-provided Subscriber key generation 17
3.6. Sub-CA-provided Subscriber key management 17
4. Certificate life cycle management 18
4.1. Certificate registration 18
4.2. External RA requirements 18
4.3. Certificate renewal 18
4.4. Certificate rekey 18
4.5. Certificate issuance 18
4.6. Certificate acceptance 18
4.7. Certificate distribution 18
4.8. Certificate revocation 18
4.9. Certificate suspension 19
4.10. Certificate status 19
4.10.1. CRL usage 19
4.10.2. OCSP usage 19
4.10.3. OCSP Designated Responder Certificates 19
4.11. Certificate profile 20
4.11.1. Apple Corporate Email Certificates 20
4.12. OCSP Designated Responder Certificate 21
4.13. CRL Profile 21

4.14. Integrated circuit cards 21
5. Environmental controls 22
5.1. CP/CPS administration 22
5.2. CA termination 22
5.3. Confidentiality 22
5.4. Intellectual property rights 23
5.5. Physical security 23
5.6. Business continuity management 23
5.7. Event logging 23
5.7.1. Archiving 23
5.7.2. Event journal reviews 23
6. Revision history 24

1. Introduction

This Certificate Policy and Certification Practice Statement ("CP/CPS") describes the practices employed by Apple in issuing and managing digital Email Certificates from dedicated Subordinate Certificates ("Apple Corporate Email Certificates Sub-CAs"), and related services.

It defines policies that Apple is required to follow. It provides additional information about the practices relating to certificate lifecycle services, such as issuance, management, revocation, renewal, and rekeying, as well as details relating to other business, legal, and technical matters specific to the Apple Corporate Email Certificates Sub-CAs, collectively referred to as the Apple Corporate Email Certificates Public Key Infrastructure ("Apple Corporate Email Certificates PKI").

1.1. Trademarks

Apple, iOS, macOS, and OS X are trademarks of Apple Inc., 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 §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
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
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, validity period, and public key.
Certification Authority	This is an entity that is authorized to issue, manage, revoke, and renew certificates under the Apple Corporate Email Certificates Sub-CAs.
Certification Authority Management Team	The group of people within Apple responsible for defining CA policy and supporting ongoing operations.
Certificate Chain	This is a collection of certificates that are considered as a group to verify the authenticity of a particular certificate. In the usual X.509 certificate model, the certificate to be verified ("leaf") is a certificate issued by a subordinate CA to a subscriber. The certificate for the subordinate CA is in turn signed by the root CA certificate. Each issued certificate contains a digital signature signed by its issuer. The digital signature can be verified at the request of a relying party so as to authenticate the source and integrity of the certificates and any objects signed or encrypted using the related public/private keys.
Certificate Policy/Certification Practice Statement	This is a corporate policy that sets forth business practices, system integrity controls, environmental controls, and specific operational practices and procedures associated with the Apple Corporate Email Certificates Sub-CAs.
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.

Term	Definition
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 a Certificate, this is a value with multiple fields that uniquely identifies each entity or resource to which a certificate is issued.
Hardware Security Module	A self-contained hardware device that provides cryptographic services used to protect an information system. Trust and integrity are derived from the security of the signing and encryption keys stored within. Cryptographic key material is securely stored within a tamper resistant (FIPS 140-2 level 3 or higher) device.
Online Certificate Status Protocol	This is a protocol that provides the ability to determine the revocation status of a digital certificate without CRLs.
Private Key	The key of a Key Pair kept secret by its holder, used to create Digital Signatures and to decrypt messages or files that were encrypted with the corresponding Public Key.
Public Key	The key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and used by the recipient to validate Digital Signatures created with the corresponding Private Key and to encrypt messages or files to be decrypted with the corresponding Private Key.
Public Key Infrastructure	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based Public Key Cryptography system.
Relying Party	This is any person or business entity that receives an X.509 certificate (issued to a subscriber by an Apple Corporate Email Certificates Sub-CA) and may rely on the validity of the certificate.
Repository	As used, same as Directory.

Term	Definition
Root Certification Authority or Root CA	This is a CA that is at the top of a hierarchical PKI network.
Subscriber	This is an end user who has been issued a Certificate signed by an Apple Corporate Email Certificates Sub-CA.
Subordinate Certification Authority or Sub-CA	This is a CA that is a node of the Root CA within a hierarchical PKI network.

2. General business practices

This section establishes and sets forth the general business practices of the Apple Corporate Email Certificates Sub-CAs.

2.1. Identification

The practices set forth in this CP/CPS apply exclusively to the Apple Corporate Email Certificates Sub-CAs. This CP/CPS discloses details of the practices employed by the Apple Corporate Email Certificates Sub-CAs in issuing Apple Corporate Email Certificates for apple.com and filemaker.com email addresses. This document assumes 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 sections of the Trust Service Principles and Criteria for Certification Authorities, a document published by the Chartered Professional Accountants of Canada ("CPA Canada") and freely available for download from their web site, www.webtrust.org. The document 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 CP/CPS, the term Apple PKI refers collectively to Apple PKI Service Providers and End Entities. Apple PKI Service Providers consist of (1) the Apple Corporate Email Certificates Sub-CAs, and their related management teams that generate, issue, distribute, revoke and manage cryptographic keys and Certificates, (2) Apple Registration Authorities ("Apple RAs"), and (3) the Apple CA Policy Authority ("Apple PA," or "PA"). End Entities are Subscribers of Certificates.

2.2. Community and applicability

This CP/CPS is applicable to Apple Corporate Email Certificates issued by an Apple Corporate Email Certificates Sub-CA with the following Certificate Policy object identifier values:

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

Policy Object Identifier Description	Policy OID
Future Use	1.2.840.113635.100.5.11.5.9

2.3. Contact details

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

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

(408) 996-1010
policy_authority@apple.com

2.4. Apportionment of liability

For Apple Corporate Email Certificates, there is not an applicable Subscriber agreement as Subscribers are internal to Apple.

2.4.1. Warranties to Subscribers and Relying Parties

There are no Subscriber agreements as all Subscribers are internal to Apple.

The Apple Corporate Email Certificates Sub-CAs do not provide warranties for any Certificate from an Apple Corporate Email Certificates Sub-CA to any Relying Party.

2.4.2. CA disclaimers of warranties

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

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

2.4.3. CA limitations of liability

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

2.4.4. Subscriber warranties

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

2.4.5. Private key compromise

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

2.4.6. Relying Party liability

Relying parties must acknowledge that they have sufficient information to make an informed decision before relying on any Apple Corporate Email Certificate, and that they are solely responsible for deciding whether or not to rely on a Certificate.

2.5. Financial responsibility

This section sets forth policies as requirements on the Apple Corporate Email Certificates Sub-CAs related to indemnification by Relying Parties and disclosure of fiduciary relationships in relying party agreements.

2.5.1. Indemnification by Subscribers

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

2.5.2. Fiduciary relationships

Not applicable.

2.6. Interpretation and enforcement

2.6.1. Governing law

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

2.6.2. Severability, survival, merger, notice

Not applicable as all Subscribers are internal to Apple.

2.6.3. Dispute resolution procedures

Any litigation or other dispute resolution related to the use of the certificates in this CPS will take place in the Northern District of California, and Relying Parties consent to the personal jurisdiction of and exclusive venue in the state and federal courts within that District with respect to any such litigation or dispute resolution.

2.7. Fees

This section sets forth policies associated with any fees charged to Subscribers for Certification Authority services for each type of Certificate.

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

The Apple Corporate Email Certificates Sub-CAs operate a private repository, which is not publicly accessible.

2.8.1. Publication of CA information

The latest version of this CP/CPS for the Apple Corporate Email Certificates Sub-CAs can be found at http://www.apple.com/certificateauthority/.

2.8.2. Frequency of publication

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

2.8.3. Access controls

There is no public repository of Certificates. Certificate status information is publicly available through OCSP and/or CRL as noted in the Certificate AIA and/or CDP extension. Apple has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

2.9. Compliance audit requirements

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 business practices disclosure and the effectiveness of the Apple Corporate Email

Certificates Sub-CAs' controls according to CPA Canada 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 CPA Canada 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 CAMT will determine the significance of identified deficiencies arising from external audits or internal self-assessments, and will prescribe remediation requirements. The CAMT will be responsible for seeing that remediation efforts are completed in a timely manner.

2.9.5. Communication of results

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

2.10. Conditions for applicability

This section sets forth practices related to the use of the Apple Corporate Email Certificates Sub-CAs.

2.10.1. Permitted uses

The Apple Corporate Email Certificates Sub-CAs may create keys, manage keys, issue Certificates, manage key life cycles, manage certificate life cycles, operate a private repository, and perform other functions to support distribution for the following types of Certificates:

- Apple Corporate Email Certificates: This type of Certificate may be used to digitally sign an email message from an authorized apple.com or filemaker.com email account, and/or encrypt a message to an authorized apple.com or filemaker.com email account, prior to delivery. For avoidance of doubt, emails associated with an Apple Corporate Email Certificate are not intended to replace a written signature or

eSignature. Apple Corporate Email Certificates are only intended to indicate that the email is from an authorized apple.com or filemaker.com email account, and does not provide any assurance of the identity of the sending party.

2.10.2. Limitations on use

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

Except for internal-use Certificates, an Apple Corporate Email Certificates Sub-CA Certificate shall not be used for any purpose that is not identified in §2.10.1 as a permitted use.

2.11. Obligations

This section sets forth policies related to the obligations of the Apple Corporate Email Certificates Sub-CAs.

2.11.1. General Sub-CA obligations

The Apple Corporate Email Certificates Sub-CAs shall:

- Conform its operations to this CP/CPS as the same may be amended from time to time.
- Issue and publish Certificates in accordance with this CP/CPS.
- Revoke Certificates issued by an Apple Corporate Email Certificates Sub-CA, 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 the Apple Corporate Email Certificates Sub-CAs.
- Publish certificate revocation information on a regular basis in accordance with this CP/CPS. As applicable, the CA shall notify the subscriber that the certificate has been revoked.

2.11.2. Notification of issuance to Subscribers

The Apple Corporate Email Certificates Sub-CAs will notify Subscribers of the issuance of certificates according to the following:

- Apple Corporate Email Certificates: Upon issuance of a certificate, the Apple Corporate Email Certificates Sub-CAs notify the Subscriber by sending notice to the email address in the Subscriber certificate.

2.11.3. Notification of issuance to others

The Apple Corporate Email Certificates Sub-CAs do not provide notification of issuance to parties other than the Subscriber.

2.11.4. Notification of revocation to Subscribers

The Apple Corporate Email Certificates Sub-CAs provide notification of certificate revocation for Subscriber initiated revocations to the Subscriber email address on record. Additionally, Certificate status information is publicly available through OCSP and/or CRL.

2.11.5. Notification of revocation to others

The Apple Corporate Email Certificates Sub-CAs do not provide notification of certificate revocation to others. Certificate status information is publicly available through OCSP and/or CRL.

2.11.6. Registration Authority obligations

A Registration Authority ("RA") external to Apple is not used. The Apple Corporate Email Certificates Sub-CAs perform limited RA services to provide reasonable assurance of the following:

- Apple Corporate Email Certificates: Certificates are issued for an apple.com or filemaker.com email addresses.

2.11.7. Subscriber obligations

Subscribers are all internal to Apple. Subscriber agreements do not exist.

2.11.8. Relying Party

Relying Parties are obligated to:

- Acknowledge that they are solely responsible for deciding whether or not to rely on the information in a Certificate, and agree that they have sufficient information to make an informed decision. Apple shall not be responsible for assessing the appropriateness of the use of a Certificate.
- Acknowledge that, to the extent permitted by applicable law, Apple hereby disclaims all warranties regarding the use of any Certificates, including any warranty of merchantability or fitness for a particular purpose. In addition, Apple hereby limits its liability, and excludes all liability for indirect, special, incidental, and consequential damages.
- Restrict reliance on Certificates issued by the CA to the purposes for which those Certificates were issued, in accordance with §2.10.1 herein, and all other applicable sections of this CP/CPS.

3. Key life cycle management

This section sets forth practices related to the key life cycle management controls of the Apple Corporate Email Certificates Sub-CAs.

3.1. Sub-CA key generation

Sub-CA signing key generation occurs using a secure cryptographic device meeting the requirements as described in §3.2.

Sub-CA signing keys are used to sign Certificates and Certificate Revocation Lists (CRLs).

The maximum lifetime of each Apple Corporate Email Certificates Sub-CA private key is fifteen (15) years.

3.2. Sub-CA private key protection

3.2.1. Sub-CA private key storage

CA private keys are stored in a Hardware Security Module (HSM) that is tamper resistant and certified at a minimum level of FIPS Level 3.

3.2.2. Sub-CA private key control

There is a separation of physical and logical access to each Apple Corporate Email Certificates Sub-CA private key, and a minimum of two individuals is required for physical access to the HSM where the Sub-CA private keys are stored.

3.2.3. Sub-CA key escrow

CA private keys shall not be placed in escrow.

3.2.4. Sub-CA key backup

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

3.2.5. Sub-CA key archival

The Apple Corporate Email Certificates Sub-CAs shall archive any necessary keys for a period of time sufficient to support the responsibilities of the Apple Corporate Email Certificates Sub-CAs.

3.3. Sub-CA public key distribution

Each Apple Corporate Email Certificates Sub-CA public key will be contained in X.509 Certificates and provided to Subscribers and Relying Parties as necessary to support the Apple Corporate Email Certificates PKI.

3.4. Sub-CA key changeover

When a new Sub-CA private key is required, a new Sub-CA Certificate will be generated. The new Apple Corporate Email Certificates Sub-CA public key Certificate will be provided to Subscribers and Relying Parties as necessary to support the Apple Corporate Email Certificates PKI.

3.5. Sub-CA-provided Subscriber key generation

The Apple Corporate Email Certificates Sub-CAs generate a Subscriber key pair and the corresponding public certificate. The key pair may be used to sign and/or encrypt an email message. The key pair is provided securely to the Subscriber via a secure mechanism.

3.6. Sub-CA-provided Subscriber key management

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

4. Certificate life cycle management

This section sets forth practices related to the certificate life cycle management controls of the Apple Corporate Email Certificates Sub-CAs.

4.1. Certificate registration

Apple Corporate Email Certificates:

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

4.2. External RA requirements

An external Registration Authority is not utilized by the Apple Corporate Email Certificates Sub-CAs.

4.3. Certificate renewal

Certificate renewal follows the same process as the initial issuance.

4.4. Certificate rekey

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

4.5. Certificate issuance

Certificates are issued to the X.509 standard. Certificates are signed using an Apple Corporate Email Certificates Sub-CA signing key. Refer to §4.12 for Certificate format, profile requirements, and required extension fields.

4.6. Certificate acceptance

Certificates shall be deemed accepted and valid immediately after issuance.

4.7. Certificate distribution

Apple Corporate Email Certificates will be distributed to the Subscriber upon issuance.

4.8. Certificate revocation

The certificate revocation process will commence upon receipt of a valid request to revoke a Certificate from the Subscriber. The Subscriber will be required to authenticate. After authentication, the Subscriber will indicate that they wish to revoke their Certificate. Once a

certificate has been revoked, its revocation status cannot be modified. An email is sent to the Subscriber to notify that the certificate has been revoked.

Certificates may be revoked by Apple for any reason.

4.9. Certificate suspension

Certificate suspension is not supported. Instead, Subscribers are required to revoke their current Certificates and request new ones.

4.10. Certificate status

The Apple Corporate Email Certificates Sub-CAs utilize two methods for certificate validation: Certificate Revocation List (CRL) and Online Certificate Status Protocol (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 for each Certificate type.

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 Corporate Email Certificates Sub-CA are used to sign all OCSP responses. More than one OCSP responder Certificate can be in operation at the same time.

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

4.10.3. 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. Apple Corporate Email Certificates

A Certificate issued by an Apple Corporate Email Certificates Sub-CA shall conform to the X.509 Certificate format and shall contain, at a minimum, the following data elements:

Field/Attribute	Value
Issuer DN	C=US, O=Apple Inc., OU= Certification Authority, CN= [*Issuing Sub-CA's Common Name*]
CRL Distribution Points and/or Certificate Authority Information Access	URL of the location where a Relying Party can check the status of a certificate.

The Apple Corporate Email Certificates also contain the following:

Field/Attribute	Critical	Value
Signature Algorithm	N/A	SHA-2 with RSA encryption
Key Usage	Yes	Digital Signature, Key Encipherment
Extended Key Usage	No	Email Protection
Basic Constraints	Yes	Certification Authority = No
Subject Alternative Name	No	Email address
Certificate Policies	No	1.2.840.113635.100.5.11.5.1

4.11.2. Apple Client Sub-CA Certificates

Apple Corporate Email Certificates Sub-CAs will conform to one of the following Subject Distinguished Name structures.

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

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

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

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

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

4.12. OCSP Designated Responder Certificate

A Certificate issued by an Apple Corporate Email Certificates 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

4.13. CRL Profile

A CRL issued by an Apple Corporate Email Certificates Sub-CA shall conform to the X.509 version 2 CRL format. Each CRL shall contain the following fields:

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

4.14. Integrated circuit cards

Not applicable.

5. Environmental controls

This section sets forth practices related to the environmental controls of the Apple Corporate Email Certificates Sub-CAs.

5.1. CP/CPS administration

Apple has designated a Policy Authority (PA) group with final authority and responsibility for specifying and approving the Apple Corporate Email Certificates CP/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 CP/CPS for the following:

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

The Apple Corporate Email Certificates Sub-CAs makes available its public CP/CPS to all Subscribers and Relying Parties, including any revisions that occur from time to time.

Any changes to the Apple Corporate Email Certificates CP/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

As set forth in this section, any decision to terminate an Apple Corporate Email Certificates Sub-CA shall be authorized by the Policy Authority prior to the effective date of termination.

Prior to the termination of the Sub-CA, Apple will develop a termination plan addressing the following:

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

5.3. Confidentiality

The Apple Corporate Email Certificates Sub-CAs shall keep the following information confidential at all times:

- All private signing and client authentication keys
- Security and annual audits and security parameters
- Security mechanisms

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

The following information shall not be considered confidential:

- Information included in Certificates
- The Apple Corporate Email Certificates Sub-CA public Certificates
- Information contained in the CA's CP/CPS document
- Any Certificate status or Certificate revocation reason code

5.4. Intellectual property rights

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

5.5. Physical security

Physical protection of equipment supporting the Apple Corporate Email Certificates PKI is achieved through the creation of clearly defined security perimeters with appropriate physical barriers to entry. Details of the physical security policies and procedures are in appropriate internal security documents.

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

5.6. Business continuity management

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

5.7. Event logging

5.7.1. Archiving

The Apple Corporate Email Certificates Sub-CAs archive 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 Apple Corporate Email Certificates Sub-CAs maintain 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 the identification and follow-up of exceptional, unauthorized, or suspicious activity.

6. Revision history

Issue Number	Issue Date	Details
1.0	March 12, 2015	Initial issuance.
2.0	April 10, 2015	Updated to include the Apple IST CA 7 – G1 Subordinate CA.
2.1	June 16, 2016	Added macOS to the Trademarks. Added Apple IST CA 6 – G1 Subordinate CA Updated font to SF Hello Thin. Updated references of WebTrust governing body to CPA Canada.
2.2	December 5, 2018	Removed specific Sub-CA names and added a separate section to provide allowed Sub-CA naming structures. Updated contact information.
2.3	June 5, 2019	Added eight new policy OIDs for future use.