Apple Inc.
Certification Authority
Certification Practice Statement
Apple Timestamp

Version 2.0
Effective Date: November 1, 2018

Table of Contents

1. Introduction

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

1.1. Trademarks

Apple, Mac, OS X, are trademarks of Apple Inc., in the United States and other countries.

1.2. Table of acronyms

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

1.3. Definitions

For the purposes of this CPS:

- "Time-stamp response" refers to a response provided by the Apple time-stamping service, which binds a representation of a datum to a particular time.

Please 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 practices of the Timestamp Sub-CA.

2.1. Identification

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

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 Timestamp 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 are Subscribers of Certificates.

The Timestamp 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 the following certificate issued by the Timestamp Sub-CA:

- Timestamp Signing Certificates: This type of Certificate may only be used by Apple to sign a time-stamp response, allowing it to be identified as a time-stamp response issued by Apple. Time-stamp responses signed by Timestamp Signing Certificates may only be used or relied upon by Apple.

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

This section is not applicable because the Subscriber and Relying Party of the Timestamp Sub-CA is Apple.

2.4.1. Warranties to Subscribers and Relying Parties

The Timestamp Sub-CA does not warrant the use of any Certificate to any Subscriber or Relying Party.

2.4.2. CA disclaimers of warranties

The Timestamp 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 Timestamp 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 as there are no Subscriber agreements since all Subscribers are internal to Apple.

2.4.5. Private key compromise

Apple reserves the right to revoke any Certificate, without notice, if it believes the private key associated with the Certificate has been compromised.

2.4.6. Subscriber and Relying Party liability

The Timestamp 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 Timestamp 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 Timestamp 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

There are no fiduciary relationships as Subscribers and Relying Parties are internal to Apple.

2.6. Interpretation and enforcement

The Timestamp 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 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 fees are charged for other CA services.

2.7.5. Refund policy

Not applicable.

2.8. Publication and Repository

The Timestamp Sub-CA operates a private repository which is not publicly accessible.

2.8.1. Publication of CA information

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

.

2.8.2. Frequency of publication

Certificate status information is made available via a Certificate Revocation List ("CRL") which is updated periodically before the CRL expiration date. Refer to the CRL Distribution Points extension for details of the CRL publication information.

2.8.3. Access controls

There is no public repository of certificates. Certificate status information is publicly available through CRL as described above. Apple has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

2.9. Compliance audit requirements

The Timestamp 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 Timestamp Sub-CA.

2.10.1. Permitted uses

The Timestamp Sub-CA will 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:

- Timestamp Signing Certificates: This type of Certificate may only be used by Apple to sign a time-stamp response, allowing it to be identified as a time-stamp response issued by Apple. Time-stamp responses signed by Timestamp Signing Certificates may only be used or relied upon by Apple.

2.10.2. Limitations on use

The Timestamp Sub-CA will not allow its Sub-CA Certificate to be used to create a certification authority or to allow its private key to sign a Certificate issued by another certification authority.

Certificates issued by the Timestamp Sub-CA shall not be used for any purpose that is not identified in this CPS § 2.10.1 as a permitted use.

2.11. Obligations

This section sets forth policies related to the obligations of the Timestamp Sub-CA.

2.11.1. General Timestamp Sub-CA obligations

The Timestamp Sub-CA shall:

- Conform its operations to the Apple CP and to this CPS as the same may be amended from time to time.
- Issue and publish Certificates in accordance with the Apple CP and this CPS.

- Revoke Certificates issued by the Timestamp Sub-CA, upon receipt of a valid request to revoke the Certificate from an authorized Subscriber. The validity of the request and the authorization of the person making the request will be determined by the Timestamp Sub-CA.
- Make certificate status information available via CRL in accordance with the Apple CP.

2.11.2. Notification of issuance to Subscribers

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

2.11.3. Notification of issuance to others

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

2.11.4. Notification of revocation to Subscribers

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

2.11.5. Notification of revocation to others

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

2.11.6. Registration Authority obligations

An external RA is not used. The Timestamp Sub-CA performs limited RA services to provide reasonable assurance that Certificates are only issued within Apple for use by Apple's time-stamping service.

2.11.7. Subscriber obligations to Sub-CA

Subscribers are obligated to:

- Safeguard their private key from compromise.
- Use their Certificates exclusively for legal purposes.
- Promptly request that the Timestamp Sub-CA revoke a Certificate if the Subscriber has reason to believe there has been a compromise of the Certificate's associated private key.
- Take no action to transfer their Certificate to any third party.

2.11.8. Relying Party obligations to Sub-CA

There are no relying party obligations as the relying parties are internal to Apple.

3. Key life cycle management

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

3.1. Sub-CA key generation

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

The Timestamp Sub-CA private key will cease to be used, and be replaced at the end of a designated period, up to a maximum of fifteen (15) years, or when a compromise is known or suspected.

3.2. Sub-CA private key protection

3.2.1. Sub-CA private key storage

Each Timestamp Sub-CA private key is stored in a Hardware Security Module (HSM) that is tamper resistant and validated at a minimum level of FIPS 140-2 Level 3.

3.2.2. Sub-CA private key control

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

3.2.3. Sub-CA key escrow

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

3.2.4. Sub-CA key backup

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

3.2.5. Sub-CA key archival

The Timestamp Sub-CA shall archive any necessary keys for a period of time sufficient to support the responsibilities of the Timestamp Sub-CA.

3.3. Sub-CA-provided Subscriber key management

The Timestamp Sub-CA does not provide Subscriber key management services.

3.4. Sub-CA public key distribution

The Timestamp Sub-CA public key will be contained in an X.509 Certificate that may be provided to Subscribers as necessary to support the Timestamp PKI.

3.5. Timestamp Sub-CA key changeover

When a new private key is required, a new Timestamp Sub-CA signing key pair will be generated and all subsequently issued certificates and CRLs are signed with the new private signing key. The corresponding new Timestamp Sub-CA public key Certificate may be provided to Subscribers as necessary to support the Timestamp PKI.

4. Certificate life cycle management

This section sets forth practices related to the certificate life cycle management controls of the Timestamp Sub-CA.

4.1. External RA requirements

An external Registration Authority is not utilized by the Timestamp Sub-CA.

4.2. Certificate registration

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

4.3. Certificate renewal

A new certificate can be issued at the request of an authorized Apple employee in accordance with internal business practices.

4.4. Certificate rekey

The Timestamp Sub-CA does not rekey certificates. Compromised keys result in completely new key sets and certificates being issued.

4.5. Certificate issuance

Certificates are issued to the ISO 9594/X.509 standard and signed using the Timestamp Sub-CA signing key.

4.6. Certificate acceptance

Upon issuance, Certificates are stored in a local repository. Certificates shall be deemed accepted and valid immediately after issuance.

4.7. Certificate distribution

Access to the local repository of certificates is granted to authorized Apple employees who administer the Timestamp Sub-CA in accordance with internal business practices.

4.8. Certificate revocation

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

Revoked certificates are noted in the Timestamp Sub-CA CRL.

4.9. Certificate suspension

Certificate suspension is not supported. New key sets and Certificates are issued if keys are compromised.

4.10. Certificate status

The Timestamp Sub-CA utilizes a published Certificate Revocation List (CRL) to provide information whether a certificate has been revoked. The CRL is updated periodically prior to the CRL expiration date.

4.11. Certificate profile

A Timestamp Signing Certificate issued by the Timestamp Authority Sub-CA 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
- Algorithm used (RSA or ECC)
- Modulus (Size in bits)
- Validity period
- Certificate Policies extension listing the CP
- Certificate qualifiers listing this CPS (URL)
- User notice qualifier
- Key Usage of Digital Signature
- Extended Key Usage extension, critical, with a purpose containing Time Stamping (2.3.6.1.5.5.7.3.8)
- CRL Distribution Points (2.5.29.31)

4.12. Integrated circuit cards

Not applicable.

5. Environmental controls

This section sets forth practices related to the environmental controls of the Timestamp Sub-CA.

5.1. CPS administration

Apple has designated a management group with final authority and responsibility for specifying and approving the Timestamp 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 Timestamp 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 Timestamp Sub-CA's CPS, along with the effective date of the changes, shall be reviewed by the PA, and posted in a timely manner.

5.2. CA termination

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

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

5.3. Confidentiality

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

- All private signing and client authentication keys
- Security and annual audits and security parameters
- Personal or non-public information about Timestamp Sub-CA Subscribers
- 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 Timestamp Sub-CA public Certificate

- Information contained in the CA's CPS and CP documents
- Any Certificate status or Certificate revocation reason code

5.4. Intellectual property rights

Certificates issued by the Timestamp Sub-CA, information provided via the CRL, the CPS and the CP are the property of Apple.

5.5. Physical security

Physical protection is achieved through the creation of clearly defined security perimeters with appropriate physical barriers to entry around the business premises and Timestamp Sub-CA facilities. 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.

Media maintained securely within the Timestamp Sub-CA facilities and is subject to the same degree of protection as the CA hardware.

At end of life, cryptographic devices are physically destroyed or zeroized in accordance to manufacturers' guidance prior to disposal.

5.6. Business continuity management

The Timestamp Sub-CA has business continuity plans to maintain or restore the Timestamp 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 Timestamp Sub-CA archives event journal data on a periodic basis.

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

5.7.2. Event journal reviews

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

Event journals are reviewed periodically.

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

6. Revision history

Issue Number	Issue Date	Details
1.0	05/18/2012	Initial release.
2.0	11/16/2018	Made changes to update contact information, certificate profile, HSM requirements, and clarify business practices.