Apple Inc.

Certification Practice Statement
Developer ID

Version 3.2

June 2, 2021

Table of Contents

1. INTRODUCTION

This Certification Practice Statement ("CPS") describes the practices employed by the Developer ID Subordinate Certification Authority ("Developer ID 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, and iOS, 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:

- "Subscriber" means a Developer or Developer's Agent who utilizes a Certificate from the Developer ID Sub-CA.
- "Developer" means an individual or organization that has registered with Apple in the Mac Developer Program and has received a Developer Identification Certificate (defined below).
- "Developer's Agent", or "Agent" means a person authorized to act for and execute responsibilities for a company (principal) when dealing with third parties. An Agent can enter into binding agreements on the principal's behalf and is responsible for any liability for the principal if the agent causes harm while carrying out his or her duties. The principal is responsible for the acts of the agent, and the agent's acts are like those of the principal.
- "Product" means a Developer application intended for use on an Apple platform.
- "Cloud Managed" refers to Certificates created and stored by Apple on behalf of an individual or company in the Developer program. The keys for these Certificates are generated and encrypted in Apple managed High Security Module (HSM). Eligible Developers can request content to be signed with the private key however, the private key cannot be extracted or copied. The Cloud Managed Certificates have an additional non-critical custom extension OID 1.2.840.113635.100.6.1.32.

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 Developer ID Sub-CA.

2.1. IDENTIFICATION

The practices set forth in this CPS apply exclusively to the Developer ID Sub-CA. This CPS is structured similarly to the CP, disclosing details of the practices employed by the Developer ID 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 Developer ID 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 Developer ID Sub-CA issues and administers Certificates in accordance with policies in the CP.

2.2. COMMUNITY AND APPLICABILITY

This CPS is applicable to the following Certificates and Cloud Managed Certificate versions indicated by an (*) issued by the Developer ID Sub-CA:

- Developer ID Installer Package Signing Certificates *
- Developer ID Application Code Signing Certificates*
- Developer ID Application and Kernel Extension Code Signing Certificates*

* Cloud Managed versions of this certificate are issued and stored as described in section 3.5 and 3.6. Cloud Managed certificates include an additional non-critical custom extension OID 1.2.840.113635.100.6.1.32 to indicate they are Cloud managed.

Certificates used exclusively for functions internal to Apple Products and/or Apple processes are not included within the scope of this CPS.

2.3. CONTACT DETAILS

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

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

(408) 996-1010
policy_authority@apple.com

2.4. APPORTIONMENT OF LIABILITY

A Subscriber agreement is incorporated in the Mac Developer Program License Agreement. There is not an applicable Relying Party agreement for Developer ID Sub-CA Certificates as the relying parties are internal to Apple. Except as provided herein, parties external to Apple are expressly prohibited from placing reliance on any aspects of the Developer ID PKI.

2.4.1. Warranties to Subscribers and Relying Parties

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

2.4.2. CA Disclaimers of Warranties

To the extent permitted by applicable law, subscriber agreements disclaim warranties from Apple, 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, subscriber agreements shall limit liability on the part of Apple and shall exclude liability for indirect, special, incidental, and consequential damages.

2.4.4. Subscriber Warranties

Subscriber agreements shall require Subscribers to warrant that:

- They will take no action to interfere with the normal operation of a Developer ID Sub-CA Certificate or products that rely on such certificates;
- They are solely responsible for preventing any unauthorized person from having access to the Subscriber's account and Subscriber's private key stored on any device for which the Subscriber is developing software for Apple platforms; and

- The Developer ID Sub-CA Certificates are being used exclusively for authorized and legal purposes.

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. 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 any digital Certificate.

2.5. FINANCIAL RESPONSIBILITY

This section sets forth policies as requirements on the Developer ID 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

Any subscriber or relying party agreement may, at Apple's discretion, include an indemnification clause by Subscribers and/or Relying Parties.

2.5.2. Fiduciary Relationships

There is no fiduciary relationship between Apple and Subscribers and/or Relying Parties.

2.6. INTERPRETATION AND ENFORCEMENT

Interpretation and enforcement of any subscriber or relying party agreement is governed by the terms and conditions in the Mac Developer Program License Agreement.

2.6.1. Governing Law

Governing law is set forth in the Mac Developer Program License Agreement.

2.6.2. Severability, Survival, Merger, Notice

Severability, survival, merger and notice if applicable, is governed by the terms and conditions in the Mac Developer Program License Agreement.

2.6.3. Dispute Resolution Procedures

Dispute resolution procedures are set forth in the Mac Developer Program License Agreement.

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. Digital certificates are available at no additional cost to members of the Mac Developer Program. Certificates are valid for their specified duration unless otherwise revoked.

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 Developer ID 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 Developer ID Sub-CA can be found at https://www.apple.com/certificateauthority.

2.8.2. Frequency of Publication

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

2.8.3. Access Controls

Subscribers shall have access to their Certificates through the Apple Developer website. There is no public repository of Subscriber certificates.

2.9. COMPLIANCE AUDIT REQUIREMENTS

The Developer ID 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 Developer ID Sub-CA.

2.10.1. Permitted Uses

The Developer ID 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 and Cloud Managed certificate versions indicated with an (*) :

- Developer ID Installer Package Certificates*: This type of Certificate may be used by Developers authorized to sign a software installer package enabling it to be installed on OS X.
- Developer ID Application Code Signing Certificates*: This type of Certificate may be used by Developers authorized to sign a software package enabling it to be run on OS X.
- Developer ID Application and Kernel Extension Code Signing Certificates*: This type of Certificate may be used by Developers authorized to sign applications and/or kernel extensions enabling them to be run on OS X.

2.10.2. Limitations on Use

The Developer ID Sub-CA will 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, the Developer ID Sub-CA Certificates shall not be used for any purpose that is not identified in this CPS § 2.10.1 as a permitted use.

2.11. OBLIGATIONS

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

2.11.1. General Developer ID Sub-CA Obligations

The Developer ID 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 Developer ID 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 Developer ID Sub-CA.
- Make certificate status information available via OCSP in accordance with the Apple CP. As applicable, the CA shall notify the subscriber that the certificate has been revoked.

2.11.2. Notification of Issuance to Subscribers

Notification to Subscribers is deemed to have taken place when newly issued Certificates are made available via the Apple Developer website, or Xcode.

2.11.3. Notification of Issuance to Others

The Developer ID Sub-CA does not provide notification of issuance to parties other than the Subscriber.

2.11.4. Notification of Revocation to Subscribers

Notification of revocation to a Subscriber is deemed to have taken place upon e-mail notification to the Subscriber.

2.11.5. Notification of Revocation to Others

The Developer ID Sub-CA does not provide notification of certificate revocation by email, except to the Subscriber. Certificate status information is publicly available through OCSP.

2.11.6. Registration Authority Obligations

An external RA is not used. The Developer ID Sub-CA performs limited RA services to provide reasonable assurance that Certificates are only issued to members of the Mac Developer Program.

2.11.7. Subscriber Obligations to Sub-CA

Subscribers are obligated to:

- Safeguard their Developer account and private key from compromise.
- Use their Certificates exclusively for legal purposes.

- Promptly request that the Developer ID Sub-CA revoke a Certificate if the Subscriber has reason to believe there has been a compromise of the Certificate's associated private key, or for any of the reasons described in the Subscriber agreement. A request for revocation is initiated by sending an email to product-security@apple.com.
- 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 Developer ID Sub-CA.

3.1. SUB-CA KEY PAIR GENERATION

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

The Developer ID Sub-CA shall sign Certificates that may be used to associate a particular Developer with a particular software application intended for use on an Apple product.

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

3.2.4. Sub-CA Key Backup

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

3.3. SUB-CA PUBLIC KEY DISTRIBUTION

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

3.4. SUB-CA KEY CHANGEOVER

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

3.5. SUBSCRIBER KEY PAIR GENERATION

When a Subscriber is signed into Xcode with their Apple ID and Password and initiates an eligible request for a new Cloud Managed certificate, a new signing key pair will be generated in an Apple managed Hardware Security Module(HSM). The corresponding public key Certificate may be provided to Subscribers via Xcode or the developer website. The Sub-CA does not provide Subscriber key pair generation for any other WWDR certificates.

3.6. SUBSCRIBER PRIVATE KEY PROTECTION

3.6.1. Subscriber Private Key Storage

Subscriber Cloud Managed private keys are generated in a Hardware Security Module (HSM) that is tamper resistant and certified at a minimum level of FIPS 140-2 Level 2. After generation, the Subscriber private key is encrypted with an additional key in the HSM and the Subscriber encrypted private key is stored in a separate database.Subscriber private key control

3.6.2. Subscriber Private Key Control

Subscriber Cloud Managed private keys are encrypted prior to storage. When WWDR receives eligible signing requests from a Subscriber, the Cloud managed encrypted private key is sent to an Apple managed HSM for decryption and processing signing requests. The decrypted private key does not leave the Apple managed HSM that is tamper resistant and certified at a minimum level of FIPS 140-2 Level 2.

4. CERTIFICATE LIFE CYCLE MANAGEMENT

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

4.1. EXTERNAL RA REQUIREMENTS

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

4.2. CERTIFICATE REGISTRATION

The issuance of a Certificate is contingent upon the requesting Subscriber being an eligible member of the Mac Developer Program. The Apple Developer website verifies that the account is one that is eligible for the issuance of Developer ID certificates and that, if applicable, Mac Developer subscription payments are current.

For Certificates that are not Cloud Managed, eligible Subscribers create a Certificate Signing Request ("CSR") using a corresponding private/public key pair generated on the client computer. Subscribers then upload completed CSRs to the Apple Developer website.

For Certificates that are Cloud Managed, eligible Subscribers request a CSR to be generated in an Apple managed High Security Module (HSM) via Xcode. The CSR is automatically requested via Xcode when initiated by an eligible Subscribe.

Upon receipt, the CSR is processed by the Apple Developer website for validity. Once the CSR is validated and a Certificate is issued by the Developer ID Sub-CA, the Subscriber is notified that the Certificate is available for download on the client computer.

The name associated with an individual Developer Identification Certificate is either the individual Subscriber's name or the Subscriber's organization name as applicable.

4.3. CERTIFICATE RENEWAL

For Certificates that are not Cloud Managed, when a Certificate expires the Subscriber will return to the Apple Developer website and submit a new CSR. This is the same process used at initial Certificate issuance.

For Cloud Managed certificates, Xcode will automatically initiate a new Certificate request when an eligible request is received from the Subscriber and the existing certificate is close to expiring or has already expired. A new certificate is generated if the Subscriber continues to be an eligible member of the Developer Program.

4.4. CERTIFICATE REKEY

The Developer ID 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, Certificates are signed using the Developer ID Sub-CA signing key.

4.6. CERTIFICATE ACCEPTANCE

Once the Developer ID Sub-CA generates a Certificate, developers will be able to download the Certificate from the Apple Developer website.

4.7. CERTIFICATE DISTRIBUTION

Certificates will be distributed to the Developer via the Apple Developer website or web services.

4.8. CERTIFICATE REVOCATION

The Subscriber may initiate a revocation request by sending an email to product-security@apple.com. The request for revocation will then be evaluated by Apple.

Certificates may be revoked by the Developer ID Sub-CA for the reasons described in the Subscriber agreement.

4.9. CERTIFICATE SUSPENSION

Certificate suspension (temporary revocation) is supported for all Developer ID Certificates. The Subscriber may initiate a suspension request by sending an email to product-security@apple.com. The request for suspension will then be evaluated by Apple. Apple can also suspend a Certificate that is supported for suspension at Apple's discretion. Once suspended, the Certificate is revoked with a reason code certificateHold. At a minimum, a Certificate may remain suspended until the certificate expiration date. A Certificate may be unsuspended at Apple's discretion as part of a re-instatement request process via the Apple Developer website.

4.10. CERTIFICATE STATUS

The Developer ID Sub-CA utilizes Online Certificate Status Protocol (OCSP) to provide information whether a certificate has been revoked. Refer to the Authority Information Access ("AIA") extensions in the Certificates for the status information method used.

4.10.1. OCSP Usage

Subscribers may use OCSP to determine the status of a particular Certificate. At a minimum, revoked Certificates remain marked as "revoked" for the Certificate lifetime with the exception of when a Certificate is unsuspended. A delegate leaf Certificate is used to sign all OCSP responses. This leaf is signed by the Developer ID Sub-CA's private key.

OSCP status requests must contain at a minimum the certificate serial number to receive a valid response. Once an OCSP request has been validated there will be a signed response back 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.

4.10.2. 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

Certificates issued by the Developer ID Sub-CA shall confirm to the X.509 version 3 Certificate format, and shall contain the following elements:

Field/Attribute	Value
Issuer DN	C = US, O = Apple Inc., OU =Apple Certification Authority, CN = Developer ID Certification Authority
CRL Distribution Points and/or Certificate Authority Information Access	URL of the location where a Relying Party can check the status of a certificate.

Individual Developer ID Sub-CA certificate profiles also contain the following:

4.11.1. Installer Package Signing Certificates

Field/ Attribute	Critical	Optional	Value
Signature Algorithm	N/A	No	SHA-2 with RSA Encryption
Key Usage	Yes	No	Digital Signature
Extended Key Usage	Yes	No	Apple Custom EKU (1.2.840.113635.100.4.13)
Custom Extensions	Yes	No	Apple Custom Extension (1.2.840.113635.100.6.1.14)
	No	Yes	Apple Custom Extension (1.2.840.113635.100.6.1.33)
	No	Yes	Apple Custom Extension (1.2.840.113635.100.6.1.32)
Basic Constraints	Yes	No	Certification Authority = No
Certificate Policy	No	No	Apple Certificate Policy (1.2.840.113635.100.5.1)

4.11.2. Application Code Signing Certificates

Field/ Attribute	Critical	Optional	Value
Signature Algorithm	N/A	No	SHA-2 with RSA Encryption
Key Usage	Yes	No	Digital Signature
Extended Key Usage	Yes	No	Code Signing (1.3.6.1.5.5.7.3.3)
Custom Extensions	Yes	No	Apple Custom Extension (1.2.840.113635.100.6.1.13)

	No	Yes	Apple Custom Extension (1.2.840.113635.100.6.1.33)
	No	Yes	Apple Custom Extension (1.2.840.113635.100.6.1.32)
Basic Constraints	Yes	No	Certification Authority = No
Certificate Policy	No	No	Apple Certificate Policy (1.2.840.113635.100.5.1)

4.11.3. Application and Kernel Extension Code Signing Certificates

Field/ Attribute	Critical	Optional	Value
Signature Algorithm	N/A	No	SHA-2 with RSA Encryption
Key Usage	Yes	No	Digital Signature
Extended Key Usage	Yes	No	Code Signing (1.3.6.1.5.5.7.3.3)
Custom Extensions	Yes	No	Apple Custom Extension (1.2.840.113635.100.6.1.13)
	Yes	No	Apple Custom Extension (1.2.840.113635.100.6.1.18)
	No	Yes	Apple Custom Extension (1.2.840.113635.100.6.1.33)
	No	Yes	Apple Custom Extension (1.2.840.113635.100.6.1.32)
Basic Constraints	Yes	No	Certification Authority = No
Certificate Policy	No	No	Apple Certificate Policy (1.2.840.113635.100.5.1)

4.12. CRL PROFILE

Not applicable.

4.13. INTEGRATED CIRCUIT CARDS

Not applicable.

5. ENVIRONMENTAL CONTROLS

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

5.1. CP & CPS ADMINISTRATION

Apple has designated a management group with final authority and responsibility for specifying and approving the Developer ID 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 Developer ID 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 Developer ID 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 Developer ID 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 Developer ID 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 Developer ID 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 Developer ID 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 Developer ID Sub-CA, information provided via the OCSP, 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 Developer ID 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 Developer ID 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 Developer ID Sub-CA has business continuity plans to maintain or restore the Developer ID 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 Developer ID 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	02/16/2012	Initial release.
1.1	06/10/2013	Updates to reflect the addition of the Application and Kernel Extension Code Signing Certificate Profile.
2.0	11/01/2018	Made changes to update contact information, HSM requirements, and clarify business practices.
2.1	03/20/2019	Annual review updates. Updated the following Certificate types: • Installer Package Signing Certificates • Application Code Signing Certificates • Application and Kernel Extension Code signing Certificates
3.0	03/27/2020	Annual review updates.
3.1	11/04/2020	Updated Certificate status and added Certificate suspension.
3.2	06/02/2021	Updated various sections related to Cloud Managed Certificates.