Apple Inc.

Apple Public Root Certification Practice Statement

Version 2.2.3

Effective Date: April 20, 2025

Table of Contents

1. INTRODUCTION 1
   1.1. OVERVIEW 1
   1.2. DOCUMENT NAME AND IDENTIFICATION 2
      1.2.1. Revisions 2
   1.3. PKI PARTICIPANTS 4
      1.3.1. Certification Authorities 4
      1.3.2. Registration Authorities 4
      1.3.3. Subscribers 4
      1.3.4. Relying Parties 5
      1.3.5. Other Participants 5
   1.4. CERTIFICATE USAGE 5
      1.4.1. Appropriate Certificate Uses 5
      1.4.2. Prohibited Certificate Uses 5
   1.5. POLICY ADMINISTRATION 6
      1.5.1. Organization Administering the Document 6
      1.5.2. Contact Person 6
      1.5.3. Person Determining CPS Suitability for the Policy 6
      1.5.4. CPS Approval Procedures 6
   1.6. DEFINITIONS AND ACRONYMS 6
      1.6.1. Definitions 6
      1.6.2. Acronyms 7
      1.6.3. References 7
      1.6.4. Conventions 7
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 9
   2.1. REPOSITORIES 9
   2.2. PUBLICATION OF CERTIFICATION INFORMATION 9
   2.3. TIME OR FREQUENCY OF PUBLICATION 9
   2.4. ACCESS CONTROLS ON REPOSITORIES 10
3. IDENTIFICATION AND AUTHENTICATION 11
   3.1. NAMING 11
      3.1.1. Types of Names 11
      3.1.2. Need for Names to be Meaningful 11
      3.1.3. Anonymity or Pseudonymity of Subscribers 11

3.1.4. Rules of Interpreting Various Name Forms....11
3.1.5. Uniqueness of Names....11
3.1.6. Recognition, Authentication, and Role of Trademarks....12
3.2. INITIAL IDENTITY VALIDATION....12
3.2.1. Method to Prove Possession of Private Key....12
3.2.2. Authentication of Organization Identity, Unique Domain Identity and Email Control12
3.2.3. Authentication of Individual Identity....17
3.2.4. Non-Verified Subscriber Information....17
3.2.5. Validation of Authority....17
3.2.6. Criteria for Interoperation....18
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS....18
3.3.1. Identification and Authentication for Routine Re-Key....18
3.3.2. Identification and Authentication for Re-Key After Revocation....18
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS....18
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS....19
4.1. CERTIFICATE APPLICATION....19
4.1.1. Who Can Submit a Certificate Application....19
4.1.2. Enrollment Process and Responsibilities....19
4.2. CERTIFICATE APPLICATION PROCESSING....20
4.2.1. Performing Identification and Authentication Functions....20
4.2.2. Approval or Rejection of Certificate Applications....21
4.2.3. Time to Process Certificate Applications....21
4.3. CERTIFICATE ISSUANCE....21
4.3.1. CA Actions During Certificate Issuance....21
4.3.2. Notification To Subscriber by the CA of Issuance of Certificate....22
4.4. CERTIFICATE ACCEPTANCE....22
4.4.1. Conduct Constituting Certificate Acceptance....22
4.4.2. Publication of the Certificate by the CA....22
4.4.3. Notification of Certificate Issuance by the CA to Other Entities....23
4.5. KEY PAIR AND CERTIFICATE USAGE....23
4.5.1. Subscriber Private Key and Certificate Usage....23
4.5.2. Relying Party Public Key and Certificate Usage....23
4.6. CERTIFICATE RENEWAL....23
4.6.1. Circumstance for Certificate Renewal....23

4.6.2. Who May Request Renewal 23
4.6.3. Processing Certificate Renewal Requests 24
4.6.4. Notification of New Certificate Issuance to Subscriber 24
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate 24
4.6.6. Publication of the Renewal Certificate by the CA 24
4.6.7. Notification of Certificate Issuance by the CA to Other Entities 24
4.7. CERTIFICATE RE-KEY 24
4.7.1. Circumstance for Certificate Re-Key 24
4.7.2. Who May Request Certification of a New Public Key 24
4.7.3. Processing Certificate Re-Keying Requests 24
4.7.4. Notification of New Certificate Issuance to Subscriber 24
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate 24
4.7.6. Publication of the Re-Keyed Certificate by the CA 24
4.7.1. Notification of Certificate Issuance by the CA to Other Entities 24
4.8. CERTIFICATE MODIFICATION 25
4.8.1. Circumstance for Certificate Modification 25
4.8.2. Who May Request Certificate Modification 25
4.8.3. Processing Certificate Modification Requests 25
4.8.4. Notification of New Certificate Issuance to Subscriber 25
4.8.5. Conduct Constituting Acceptance of Modified Certificate 25
4.8.6. Publication of the Modified Certificate by the CA 25
4.8.7. Notification of Certificate Issuance by the CA to Other Entities 25
4.9. CERTIFICATE REVOCATION AND SUSPENSION 25
4.9.1. Circumstances for Revocation 25
4.9.2. Who Can Request Revocation 29
4.9.3. Procedure for Revocation Request 29
4.9.4. Revocation Request Grace Period 30
4.9.5. Time Within Which CA Must Process the Revocation Request 30
4.9.6. Revocation Checking Requirement for Relying Parties 30
4.9.7. CRL Issuance Frequency 30
4.9.8. Maximum Latency for CRLs 31
4.9.9. On-Line Revocation/Status Checking Availability 31
4.9.10. On-Line Revocation Checking Requirements 31
4.9.11. Other Forms of Revocation Advertisements Available 32

4.9.12. Special Requirements Re Key Compromise 32
4.9.13. Circumstances for Suspension 33
4.9.14. Who Can Request Suspension 33
4.9.15. Procedure for Suspension Request 33
4.9.16. Limits on Suspension Period 33
4.10. CERTIFICATE STATUS SERVICES 33
4.10.1. Operational Characteristics 33
4.10.2. Service Availability 33
4.10.3. Operational Features 33
4.11. END OF SUBSCRIPTION 33
4.12. KEY ESCROW AND RECOVERY 33
4.12.1. Key Escrow and Recovery Policy and Practices 33
4.12.2. Session Key Encapsulation and Recovery Policy and Practices 34
5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS 35
5.1. PHYSICAL security CONTROLS 35
5.1.1. Site location and construction 35
5.1.2. Physical Access 35
5.1.3. Power and Air Conditioning 35
5.1.4. Water Exposures 35
5.1.5. Fire Prevention and Protection 35
5.1.6. Media Storage 36
5.1.7. Waste Disposal 36
5.1.8. Off-Site Backup 36
5.2. PROCEDURAL CONTROLS 36
5.2.1. Trusted Roles 36
5.2.2. Number of Persons Required per Task 37
5.2.3. Identification and Authentication for Each Role 37
5.2.4. Roles Requiring Separation of Duties 37
5.3. Personnel CONTROLS 37
5.3.1. Qualifications, Experience, and Clearance Requirements 37
5.3.2. Background Check Procedures 38
5.3.3. Training Requirements and Procedures 38
5.3.4. Retraining Frequency and Requirements 38
5.3.5. Job Rotation Frequency and Sequence 39

5.3.6. Sanctions for Unauthorized Actions 39
5.3.7. Independent Contractor Requirements 39
5.3.8. Documentation Supplied to Personnel 39
5.4. AUDIT LOGGING PROCEDURES 39
5.4.1. Types of Events Recorded 39
5.4.2. Frequency of Processing and Archiving Audit Logs 40
5.4.3. Retention Period for Audit Logs 40
5.4.4. Protection of Audit Log 41
5.4.5. Audit Log Backup Procedures 41
5.4.6. Audit Collection System (Internal Vs. External) 41
5.4.7. Notification To Event-Causing Subject 41
5.4.8. Vulnerability Assessments 41
5.5. RECORDS ARCHIVAL 41
5.5.1. Types of Records Archived 41
5.5.2. Retention Period for Archive 42
5.5.3. Protection of Archive 43
5.5.4. Archive Backup Procedures 43
5.5.5. Requirements for Time-Stamping of Records 43
5.5.6. Archive Collection System (Internal or External) 43
5.5.7. Procedures to Obtain and Verify Archive Information 43
5.6. KEY CHANGEOVER 43
5.7. COMPROMISE AND DISASTER RECOVERY 44
5.7.1. Incident and Compromise Handling Procedures 44
5.7.2. Computing Resources, Software, and/or Data Are Corrupted 44
5.7.3. Entity Private Key Compromise Procedures 44
5.7.4. Business Continuity Capabilities After a Disaster 44
5.8. CA OR RA TERMINATION 45
6. TECHNICAL SECURITY CONTROLS 46
6.1. KEY PAIR GENERATION AND INSTALLATION 46
6.1.1. Key Pair Generation 46
6.1.2. Private Key Delivery to Subscriber 47
6.1.3. Public Key Delivery to Certificate Issuer 47
6.1.4. CA Public Key Delivery to Relying Parties 47
6.1.5. Key Sizes 47

6.1.6. Public Key Parameters Generation and Quality Checking 48
6.1.7. Key Usage Purposes (as per X.509 v3. Key Usage Field) 48
6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 49
6.2.1. Cryptographic Module Standards and Controls 49
6.2.2. Private Key (n out of m) Multi-Person Control 49
6.2.3. Private Key Escrow 49
6.2.4. Private Key Backup 49
6.2.5. Private Key Archival 49
6.2.6. Private Key Transfer Into or From a Cryptographic Module 49
6.2.7. Private Key Storage on Cryptographic Module 49
6.2.8. Method of Activating Private Key 49
6.2.9. Method of Deactivating Private Key 50
6.2.10. Method of Destroying Private Key 50
6.2.11. Cryptographic Module Rating 50
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT 50
6.3.1. Public Key Archival 50
6.3.2. Certificate Operational Periods and Key Pair Usage Periods 50
6.4. ACTIVATION DATA 50
6.4.1. Activation Data Generation and Installation 50
6.4.2. Activation Data Protection 51
6.4.3. Other Aspects of Activation Data 51
6.5. COMPUTER SECURITY CONTROLS 51
6.5.1. Specific Computer Security Technical Requirements 51
6.5.2. Computer Security Rating 51
6.6. LIFE CYCLE TECHNICAL CONTROLS 51
6.6.1. System Development Controls 51
6.6.2. Security Management Controls 52
6.6.3. Life Cycle Security Controls 52
6.7. NETWORK SECURITY CONTROLS 52
6.8. TIME-STAMPING 52
7. CERTIFICATE, CRL, AND OCSP PROFILES 53
7.1. CERTIFICATE PROFILE 53
7.1.1. Version Numbers 53

7.1.2. Certificate Content and Extensions 53
7.1.3. Algorithm Object Identifiers 66
7.1.4. Name Forms 66
7.1.5. Name Constraints 70
7.1.6. Certificate Policy Object Identifier 70
7.1.7. Usage of Policy Constraints Extension 73
7.1.8. Policy Qualifiers Syntax and Semantics 73
7.1.9. Processing Semantics for the Critical Certificate Policies Extension 73
7.2. CRL PROFILE 74
7.2.1. Version Number 75
7.2.2. CRL and CRL Entry Extensions 75
7.3. OCSP PROFILE 76
7.3.1. Version Number 76
7.3.2. OCSP Extensions 77
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 78
8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 78
8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR 78
8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 78
8.4. TOPICS COVERED BY ASSESSMENT 78
8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY 78
8.6. COMMUNICATION OF RESULTS 79
8.7. SELF-AUDITS 79
8.8. Review of delegated parties 79
9. OTHER BUSINESS AND LEGAL MATTERS 80
9.1. FEES 80
9.1.1. Certificate Issuance or Renewal Fees 80
9.1.2. Certificate Access Fees 80
9.1.3. Revocation or Status Information Access Fees 80
9.1.4. Fees for Other Services 80
9.1.5. Refund Policy 80
9.2. FINANCIAL RESPONSIBILITY 80
9.2.1. Insurance Coverage 80
9.2.2. Other Assets 80
9.2.3. Insurance or Warranty Coverage for End-Entities 80

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION 81
9.3.1. Scope of Confidential Information 81
9.3.2. Information Not Within the Scope of Confidential Information 81
9.3.3. Responsibility To Protect Confidential Information 81
9.4. PRIVACY OF PERSONAL INFORMATION 81
9.4.1. Privacy Plan 81
9.4.2. Information Treated as Private 81
9.4.3. Information Not Deemed Private 82
9.4.4. Responsibility To Protect Private Information 82
9.4.5. Notice and Consent To Use Private Information 82
9.4.6. Disclosure Pursuant to Judicial or Administrative Process 82
9.4.7. Other Information Disclosure Circumstances 82
9.5. INTELLECTUAL PROPERTY RIGHTS 82
9.6. REPRESENTATIONS AND WARRANTIES 82
9.6.1. CA Representations and Warranties 82
9.6.2. RA Representations and Warranties 83
9.6.3. Subscriber Representations and Warranties 83
9.6.4. Relying Party Representations and Warranties 84
9.6.5. Representations and Warranties of Other Participants 85
9.7. DISCLAIMERS OF WARRANTIES 85
9.8. LIMITATIONS OF LIABILITY 85
9.9. INDEMNITIES 86
9.9.1. Indemnification by Apple 86
9.9.2. Indemnification by Subscribers 86
9.9.3. Indemnification By Relying Parties 87
9.10. TERM AND TERMINATION 87
9.10.1. Term 87
9.10.2. Termination 87
9.10.3. Effect of Termination and Survival 87
9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 88
9.12. AMENDMENTS 88
9.12.1. Procedure for Amendment 88
9.12.2. Notification Mechanism and Period 88
9.12.3. Circumstances Under Which OID Must Be Changed 88

9.13. DISPUTE RESOLUTION PROVISIONS 88
9.14. GOVERNING LAW 88
9.15. COMPLIANCE WITH APPLICABLE LAW 89
9.16. MISCELLANEOUS PROVISIONS 89
9.16.1. Entire Agreement 89
9.16.2. Assignment 89
9.16.3. Severability 89
9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights) 89
9.16.5. Force Majeure 89
9.17. OTHER PROVISIONS 89
Appendix A: Apple Root and Subordinate CAs Hierarchy 90
Appendix B: Verification Sources 92
Sources List 92
Revision History 92
Appendix C - Registration Schemes for Organization Identifier in S/MIME Certificates 93
Appendix D - Revocation Reason Code Selection 94

1. INTRODUCTION

1.1. OVERVIEW

This Certification Practice Statement ("CPS") describes the practices employed by Apple Inc. ("Apple") acting as a Root CA and Subordinate CA that issues Publicly-Trusted Certificates ("Apple Public CA").

Root Certificates issued by the Apple Public CA are intended to be widely trusted by Application Software Suppliers. As such, the Apple Public CA inherits the benefits and responsibilities associated with those Application Software Suppliers' programs, which are listed in Section 1.1. of the Apple Public Root Certificate Policy ("Apple Public Root CP").

The Apple Public CA issues Root Certificates and Subordinate CA Certificates ("Sub-CA Certificate") for Apple Inc. and its subsidiaries. Appendix A lists all valid Root Certificates and associated Sub-CA Certificates.

The Apple Public CA also issues Subscriber Certificates and manages related services to:

- Secure connections based on the TLS protocol, and
- Digitally sign and encrypt email using the S/MIME standard.

This CPS provides the practices for issuance of all Certificates, including Root Certificates, Sub-CA Certificates and Subscriber Certificates, including Organization Validated ("OV") TLS Server Certificates, as well as Mailbox-validated and Organization-validated S/MIME Certificates. This CPS further defines the practices relating to Certificate lifecycle services, such as issuance, management, and revocation, as well as details relating to other business, legal, and technical matters.

Any practice that is designed for a specific Certificate type is explicitly identified. Those practices are designed to conform to the requirements in the current version of the Apple Public Root CP. The Apple Public CA includes policy identifiers in Certificates as discussed in Section 7.1.6, to assert that Apple makes commercially reasonable efforts to conform to the CAB Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this CPS and the Apple Public Root CP, the Apple Public Root CP takes precedence. The CAB Forum Baseline Requirement takes precedence over the Apple Public Root CP.

This CPS is structured according to RFC 3647, and includes at least every section and subsection defined in RFC 3647. There are sections that include the words "No Stipulation", which mean that no specific practices exist for that section. This CPS contains no sections that are blank.

1.2. DOCUMENT NAME AND IDENTIFICATION

This is the Apple Public Root CPS. The name reflects the publicly-trusted nature of the Certification Authority regulated by it. This CPS has been assigned this Object Identifier within the applePublicPolicyID:

aprCPSroot ::= {applePublicPolicyID (1) aprCPS (2) 1} — (1.2.840.113635.100.5.19.1.2.1)

This and other Apple-owned arcs are used in the certificate policies extension as described in Section 7.1.6.

1.2.1. Revisions

This CPS is reviewed and updated at least annually, as required by the Baseline Requirements.

The following revisions have been made to the original document:

Date	Changes	Version
04/20/2025	Updated Sections 4.6, 4.9.12 and 6.1.1.3 to allow Certificate renewal and provide flexibility in the management of compromised keys.	2.2.3
03/07/2025	Updated Section 3.2.2.4 to limit the use of method 2 and add CNAME option to method 7. Updated Sections 1.6.2, 3.2.2.4 and 3.2.2.8 to incorporate enhanced DNS record verification using multiple perspectives. Updated Appendix A to include newly issued Subordinate CA Certificates' information.	2.2.2
12/05/2024	Updated Section 4.9.7 to make the practice more flexible.	2.2.1
09/15/2024	Updated Sections 3.2.2.8, and 4.2.1 to include practices for CAA for S/MIME. Updated Section 3.2.2.10 to remove Wildcard Certificates' manual approval and more accurately describe the high risk certificate's practice. Updated Appendix A to include new Subordinate CA Certificates' information for replacements of S/MIME Extant CAs.	2.2
03/15/2024	Updated multiple sections to bring the document to compliance with Baseline Requirements up to version 2.0.2. including: 4.9.7, 4.9.9, 4.9.10, 7.1.2.6, 7.1.2.7, 7.1.2.8, 7.1.2.11, 7.2, 7.2.1, 7.2.2, and Appendix D. Updated self-audit practices for SMIME Certificates in Section 8.7. Made editorial updates in Sections 1.3.3, 1.3.4, 3.1.2, 3.1.3, 5.1 and 7.3.1. Multiple other Sections updated for TLS Server Certificates.	2.1
09/01/2023	Updated multiple sections to bring the document to compliance with Baseline Requirements up to version 2.0. and S/MIME Baseline Requirements up to version 1.0.1.	2.0

Date	Changes	Version
11/15/2022	Updated multiple sections to clarify and refine some practices based on Application Software Suppliers' requirements: Section 1.4.2 - added prohibited used related to surreptitious interception and clarified existing sentence. Section 1.5.2.1 - included location for Certificate Problem Reporting instructions. Section 2.3 - added practice of publishing CP to the CCADB within seven calendar days of approval and changed business day for calendar days. Section 3.2.5 - established the connection between Reliable Communication Methods and authority validation. Made editorial change to separate subsection. Section 4.3.1 - expanded on actions executed during certificate creation and clarified the publishing of Precertificates to Certificate Transparency logs. Section 4.9 - added the notion of Precertificate revocation and revocation status. Section 4.9.1.2 (5) - added "the Apple Public Root CP" for completeness. Section 4.9.3 - clarified practice around Certificate Problem Reporting for external parties. Section 5.3.7 - clarified training practices for contractors. Section 5.4.1 - explained that automated and manual event collection processes are used.	1.4
10/01/2022	Updated Sections 2.1, 4.3.1, 4.9.3, 4.9.9, 4.9.12, 6.1.1.3, 7.2, 7.3.1, 8.2, 8.6, 9.6.3, and added Appendix D for compliance with Mozilla Root Store Policy version 2.8. Updated Section 4.9.9 for compliance with Apple Root Certificate Program. Updated Appendix B - Verification Sources to include new verification website. Made minor editorial changes to Section 7.1.2, 7.1.4.3, 7.2.1, and 9.6.3.	1.3
09/01/2022	Updated Sections 3.2.2.4, 3.2.2.8, 4.1.1, 5.4.1, 5.4.2, 5.4.3, 5.4.6, 5.5.1, and 5.5.2 to comply with Apple Public Root CP version 1.1 (for compliance with CABF Baseline Requirement up to version 1.8.4) Updated Sections 5.2.1.4, 5.2.2 and 5.3.7 to expand certain Trusted Roles to contractors. Updated section 4.9.7 to simplify CRL issuance frequency language, Section 5.1.4 to better reflect water protection practices in diverse facilities. Updated Sections 3.2.2.6, 3.2.2.10 to use defined terms and amend Wildcard Certificates practice. Updated Sections 5.1.1, 5.1.8, 5.4.4., 5.4.5, 5.5.3 and 5.5.4 to better reflect log recording and archival practices. Updated Section 5.4.8 to reflect vulnerability assessment practices. Updated Section 9.14 to change governing law.	1.2

Date	Changes	Version
01/14/2022	Updated Appendix A with the Root Certificate and Sub-CA Certificate serial numbers.	1.1
12/09/2021	Initial release.	1.0

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

A Certification Authority ("CA") is an organization that is authorized to issue, manage, and revoke Certificates. The Apple Public CA acts as the Root CA and Subordinate CA for Apple.

1.3.2. Registration Authorities

A Registration Authority ("RA") performs identification and authentication checks for end-user Certificate applicants. The Apple Public CA acts as a Registration Authority. This function is not delegated to a third party.

1.3.2.1. Enterprise Registration Authorities

The Apple Public CA may delegate to an Enterprise Registration Authority ("Enterprise RA") responsibilities related to the verification of information in its own organization's Certificate Applications. Prior to allowing this delegation, the Apple Public CA:

1. For Mailbox-validated and Organization-validated Certificate Applications, verifies that the Enterprise RA has authorization or control over the domain component for the Certificate Applications submitted in accordance with Section 3.2.2.9.

2. For Organization-validated Certificate Applications, verifies the name included in the subject:organizationName is either of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject in accordance with Section 3.2.2.1.

These restrictions are outlined in the Terms of Use or Subscriber Agreement signed by the Applicant/Subscriber and are monitored for compliance in accordance with Section 8.8.

1.3.3. Subscribers

A Subscriber is a natural person or Legal Entity that has been issued a Certificate signed by an Apple Public CA Certificate and is legally bound by a Subscriber Agreement or Terms of Use. In some situations, a CA acts as an Applicant or Subscriber, for instance, when it generates and protects a Private Key, requests a Certificate, demonstrates control of a Domain, or obtains a Certificate for its own use.

1.3.4. Relying Parties

A Relying Party is any natural person or Legal Entity that relies on a Valid Certificate issued by the Apple Public CA.

1.3.5. Other Participants

1.3.5.1. CAB Forum

See the Apple Public Root CP Section 1.3.5.1 for details

1.3.5.2. Application Software Supplier

See the Apple Public Root CP Section 1.3.5.2 for details

1.3.5.3. Apple CA Policy Authority

The Apple Policy Authority (APA) is a multi-disciplinary group from within Apple Inc., and its subsidiaries responsible for interpretation of requirements, maintenance, and approval of this CPS.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate Certificate Uses

1.4.1.1. TLS Server and Client Certificates

The Apple Public CA issues and administers X.509 Certificates with Server Authentication and/or Client Authentication purposes used to provide server authentication, data encryption, message integrity, and, optionally, client authentication.

1.4.1.2. S/MIME Certificates

The Apple Public CA issues and administers X.509 Certificates with an Email Protection purpose used to provide secure email. This type of Certificate can be used to digitally sign and/or encrypt an email message. S/MIME Certificates are intended only to indicate that the email message is from an authorized email account, but do not provide any assurance of the identity of the sending party. Further, email messages associated with an S/MIME Certificate are not intended to replace a written or electronic signature.

1.4.2. Prohibited Certificate Uses

The Apple Public CA does not allow its Subscribers' Certificates to sign other Certificates, nor does it allow its Sub-CA Private Keys to sign other Sub-CA Certificates.

Subscriber Certificates may not be used for the purpose of intercepting encrypted network traffic (e.g. "man-in-the-middle attacks").

Certificates issued by the Apple Public CA shall not be used for any purpose that is not identified in Section 1.4.1 as a permitted use.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

This CPS is administered by the APA.

1.5.2. Contact Person

The contact information for this CPS is:

Apple CA Policy Authority
One Apple Park Way
Cupertino, CA 95014

(408) 996-1010
policy_authority@apple.com

1.5.2.1. Certificate Problem Reporting

To submit a Certificate Problem Report, there are two mechanisms:

- Relying Parties, Application Software Suppliers, and other third parties contact us at contact_pki@apple.com. Instructions on how to submit a Certificate Problem Report are provided on https://www.apple.com/certificateauthority/public.
- Staff of Apple Inc. and its subsidiaries, use mechanisms available through the Certificate Enrollment system.

1.5.3. Person Determining CPS Suitability for the Policy

The APA determines the suitability and applicability of this CPS. The APA considers, among other factors, the results and observations received from independent auditors as specified in Section 8, internal auditors, and Application Software Suppliers.

1.5.4. CPS Approval Procedures

This CPS and all its amendments are subject to approval by the APA. The CPS may change at any time without prior notice. Amendments to this CPS will be evidenced by a new version number and date and recorded in the revision table in Section 1.2.1, except where the amendments are purely clerical.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

This CPS adopts the Apple Public Root CP Appendix C definitions. References not included in the Apple Public Root CP are listed below.

Term	Definition
A-Label	From RFC 5890 (http://tools.ietf.org/html/rfc5890): A Domain Label that starts with the characters "xn--" followed by a string that is a valid output of the Punycode algorithm and hence a maximum of 59 ASCII characters in length.
Certificate Application	The document, physical or electronic, submitted by an Applicant to Apple Public CA for the purpose of obtaining a Certificate.
Certificate Requester	A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an Certificate Application on behalf of the Applicant.
Distinguished Name	Within the scope of a CA related to the issuance and management of Certificates, this is a value that uniquely identifies each entity or resource to which a Certificate is issued.
Identification Credential	A cryptographic-based identity that uniquely identifies a staff member of Apple Inc., or one of its subsidiaries. The Identification Credential is associated with information such as the staff member's name and email address.
Internationalized Domain Name	From RFC 5890 (http://tools.ietf.org/html/rfc5890): A Domain Name that contains at least one A-label or U-label, but that otherwise may contain any mixture of LDH Label, Non-Reserved LDH labels, A-labels, or U-labels.
U-Label	From RFC 5890 (http://tools.ietf.org/html/rfc5890): A string of Unicode characters including at least one non-ASCII character, expressed in a standard Unicode Encoding Form (such as UTF-8).

1.6.2. Acronyms

This CPS adopts the Apple Public Root CP Appendix C acronyms. Acronyms not included in the Apple Public Root CP are listed below.

Acronym	Term
DN	Distinguished Name
IDN	Internationalized Domain Name
RRset	Resource Record Set

1.6.3. References

This CPS adopts the Apple Public Root CP Section 1.6.3 references. References not included in the Apple Public Root CP will be listed below.

1.6.4. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in the policies, guidelines, and requirements mentioned in Section 1.1. have been interpreted in accordance with RFC 2119.

By convention, this CPS omits time and timezones when listing effective requirements such as dates. Except when explicitly specified, the associated time with a date is 00:00:00 UTC.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

The Apple Public CA repository is composed of multiple private and public areas as described below:

- Subscriber Certificates are placed in an area not publicly accessible. TLS Server Certificates intended to operate with Apple and Google clients are published to publicly accessible Certificate Transparency logs.
- Status information for Subscriber Certificates is available from publicly accessible locations linked from the Subscriber Certificate.
- Root Certificates and Sub-CA Certificates are available on publicly accessible websites.
- The current version, and previous versions, of the Apple Public Root CP, and this CPS, are made available on publicly accessible websites.
- Standard agreements and other policies (e.g. Privacy Policy) are made available on publicly accessible websites.
- Results of the annual audit are made available on publicly accessible websites.

Modifications to this CPS will be logged in the Revisions table in Section 1.2.1 by increasing the CPS version and referencing the source of the requirement. If a full year passes without any changes to this document, a new dated entry and increased version number will be logged to note compliance with the requirement of an annual review.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

The latest versions of the Apple Public Root CP, this CPS and agreements are published at https://www.apple.com/certificateauthority/public and are readily accessible on a 24x7 basis. The Apple privacy policy is available at https://www.apple.com/legal/privacy

Links to test web pages used to demonstrate valid, revoked, and expired Certificates are available from pages linked from https://www.apple.com/certificateauthority/public.

Certificate status information may be made available through the Online Certificate Status Protocol ("OCSP"). Certificate status information may also be checked via the Certificate Revocation List ("CRL"), which is published by the Apple Public CA on a periodic basis. Refer to the CRL Distribution Point or the Authority Information Access extensions in the Certificates for the status information method used as described in Section 7.1.2.

2.3. TIME OR FREQUENCY OF PUBLICATION

The Apple Public CA has a process in place to develop, implement, and enforce, any new requirements set forth by the CAB Forum in the Baseline Requirements, the S/MIME Baseline Requirements, and by Application Software Suppliers. This process is triggered

at least every quarter and relies on monitoring the CAB Forum and Application Software Supplier websites for document changes and newly approved ballots.

Updates to this CPS and updated agreements are published to the Repository as necessary, but within seven (7) calendar days after approval. Updated versions of this CPS are uploaded to the CCADB within seven (7) calendar days after approval.

Certificate status information for Subscriber Certificates is published as specified in Section 4.9.7 for CRLs and Section 4.9.10 for OCSP.

Root Certificates and Sub-CA Certificates are published as soon as possible after issuance.

2.4. ACCESS CONTROLS ON REPOSITORIES

Read-only access to information in public repositories is provided without restriction. Read-only access to Certificates in private repositories is available through an internal process.

The Apple Public CA has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

Certificates contain a Subject defined in Section 7.1.2.7; and, a Subject Alternative Name extension defined in Section 7.1.4.4.

3.1.2. Need for Names To Be Meaningful

All Certificates include a non-null Issuer Distinguished Name ("Issuer DN") containing information about Apple Inc., the issuer of the Certificate.

TLS Server Certificates include a non-null Subject DN containing the verified information of an entity (i.e. Subscriber), which is either Apple Inc. or one of its subsidiaries. The Fully Qualified Domain Names ("FQDN") and/or Wildcard Domain Names included in the Subject Alternative Name extension and Common Name field identify the device(s) controlled by the Subscriber. For IDNs, the Apple Public CA may include the Punycode version of the IDN as a subject name

S/MIME Certificates include a non-null Subject DN containing either the verified information of an entity (i.e. Subscriber), which is either Apple Inc. or one of its subsidiaries, and the verified Mailbox; or, the verified Mailbox Address only in either the Common Name or Email Address fields. The rfc822Name field in the Subject Alternative Name extension includes the Mailbox Address from the Subject DN.

3.1.3. Anonymity Or Pseudonymity Of Subscribers

Generally, the Apple Public CA does not issue Certificates with pseudonyms.

3.1.4. Rules of Interpreting Various Name Forms

Distinguished names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.4.1. Non ASCII Character Substitution

The Apple Public CA will convert Subject Identity Information (i.e., Organization name) rendered in non-ASCII to the equivalents shown below. This conversion will be carried out as part of the verifications performed in Section 3.2.2.1 and 3.2.2.2:

3.1.4.2. Geographic Names

The Apple Public CA will use geographic endonyms and exonyms in the subject:localityName and subject:stateOrProvinceName attributes and avoid the use archaic geographic names, when appropriate. This use will be evaluated during verifications performed in Section 3.2.2.1 and 3.2.2.2.

3.1.5. Uniqueness of Names

The uniqueness of each subject name in a Certificate is enforced as follows:

Certificate Type	Uniqueness Determination
Root Certificate	Root CA organization's name combined with its headquarters' country.
Sub-CA Certificate	Subordinate CA organization's name combined with its headquarters' country.
TLS Server Certificate	Domain Validated: Domain Name, whose uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers ("ICANN") Organization Validated: The combination of Subscriber's organization name and headquarters' location, which may include locality, state/province and country.
S/MIME Certificate	Mailbox-validated: A verified unique Mailbox Address. Organization-validated: The combination of a unique Mailbox Address and the organization's name.

3.1.6. Recognition, Authentication, and Role of Trademarks

Apple, iOS, and macOS are trademarks of Apple Inc., in the United States and other countries.

Applicants are prohibited from requesting Certificates that contain content which infringes on the intellectual property and commercial rights of others. The Apple Public CA does not determine whether Applicants have intellectual property rights in the name used in a Certificate Application nor does the Apple Public CA resolve any dispute concerning the ownership of a domain name or trademark. The Apple Public CA may reject any Certificate Application and revoke any Certificate because of such a dispute.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Method To Prove Possession of Private Key

The Certificate Applicant must demonstrate that it rightfully holds the Private Key corresponding to the Public Key listed in the Certificate by submitting a PKCS#10 Certificate Signing Request ("CSR").

3.2.2. Authentication of Organization Identity, Unique Domain Identity and Email Control

Information to be included in a Certificate's Subject DN is validated as explained in the following sections.

3.2.2.1. Authentication of Organization Identity

For Certificates whose Applicant is a Legal Entity, the Apple Public CA confirms that the Applicant, the Applicant's jurisdiction of incorporation, registration, or place of business is not on any United States Government denied list, list of prohibited persons, or other list that prohibits doing business with such organization.

The Apple Public CA collects and retains evidence supporting the following identity attributes for the Organization:

- Formal name of the Legal Entity,
- A registered Assumed Name for the Legal Entity (if included in the Subject),
- An address of the Legal Entity (if included in the Subject),
- Jurisdiction of Incorporation or Registration of the Legal Entity, and
- Unique identifier and type of identifier for the Legal Entity.

While multiple registration schemes for the verification of the organizationIdentifier may be used (See: Appendix C), the Apple Public CA prefers the Legal Entity Identifier ("LEI") scheme when possible.

When an Attestation Letter or Verified Professional Letter is provided as part of the process, such letter is verified in accordance with Section 3.2.2.7.

TLS Server Certificates and Organization-Validated S/MIME Certificates

The Apple Public CA verifies the full legal name and address using documentation provided by, or through communication with, at least one of the following as described in Baseline Requirements Section 3.2.2.1:

1. A government agency in the jurisdiction of the Legal Entity's legal creation, existence, or recognition as listed in Appendix B, or
2. A third party database that is periodically updated and considered a Reliable Data Source, or
3. A site visit by a representative of the Apple Public CA, or
4. An Attestation Letter provided by the Applicant, or
5. (Only for Organization-validated S/MIME Certificates) A Legal Entity Identifier data reference. When LEI data reference is used, the Apple Public CA verifies that the RegistrationStatus is ISSUED and the EntityStatus is ACTIVE. The Apple Public CA only allows use of an LEI if the ValidationSources entry is FULLY_CORROBORATED. The country code used in the Registration Scheme identifier is confirmed to match that of the subject:countryName for the specific Legal Entity being verified.

Mailbox-Validated S/MIME Certificates

Apple Public CA verifies the Mailbox Address to be included in an rfc822Name field in the Subject Alternative Extension, Email Address or Common Name fields in the Subject DN, using the practices in Section 3.2.2.9.

3.2.2.2. DBA/Tradename

When the Subject Identity Information includes a DBA or trademark, the Apple Public CA uses a method below to perform the verification.

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition,
2. A Reliable Data Source,
3. Communication with a government agency responsible for the management of such DBAs or tradenames,
4. An Attestation Letter accompanied by documentary support, or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the Apple Public CA determines to be reliable.

3.2.2.3. Verification of Country

When countryName is included in a Certificate, the Apple Public CA verifies it using Section 3.2.2.1.

3.2.2.4. Validation of Domain Authorization or Control

Prior to issuance of a TLS Server Certificate, the Apple Public CA validates each FQDN to be included in such Certificates. As part of the validation process, the Apple Public CA records the validation method, and the associated Baseline Requirements' version.

Validation of FQDNs is performed using these methods described in the Baseline Requirements sections:

- (3.2.2.4.2) – Email, Fax, SMS, or Postal Mail to Domain Contact, by sending a Random Value via email to the Domain Contact, and receiving a confirming response utilizing the Random Value within 20 days of its generation. This method, and any information produced by it, will no longer be used after July 10, 2025.
- (3.2.2.4.7) – DNS Change, by confirming the presence of a CA-generated Random Value in either a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character. Confirmation is completed within 20 days of generation of the Random Value. DNS RRsets will be corroborated as described in Section 3.2.2.8.

FQDNs are also reviewed to prevent use of Internal Names.

The Apple Public CA does not issue Certificates with the Onion Domain Names nor with mixed character sets.

3.2.2.5. Authentication for an IP Address

The Apple Public CA does not issue TLS Server Certificates containing IP Addresses.

3.2.2.6. Wildcard Domain Validation

Every Wildcard Domain Name in a Certificate Application is verified before issuing a Wildcard Certificate. The Wildcard Domain Name's Base Domain Name part is compared with Domain Names in the "ICANN DOMAINS" section of the Public Suffix List. When none of those FQDNs is present in the list, the Certificate may be issued. When the FQDN is present in the list, additional information is requested from the Applicant to verify ownership before the Certificate can be issued.

3.2.2.7. Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the Apple Public CA considers the following during its evaluation:

- The age of the information provided,
- The frequency of updates to the information source,
- The data provider and purpose of the data collection,
- The public accessibility of the data availability, and
- The relative difficulty in falsifying or altering the data.

The Apple Public CA does not use its own databases as a Reliable Data Sources.

3.2.2.8. CAA Records

Prior to issuing a TLS Server or S/MIME Certificate, the Apple Public CA determines the Relevant RRset for each Domain Name in the Certificate Application.

As of March 15, 2025, Apple Public CA corroborates the Primary Network Perspective with no less than two additional Remote Network Perspectives. Communications between the Remote Network Perspectives and the Apple Public CA are over HTTPS. A Certificate is issued regardless of the number of "non-corroborations".

For TLS Certificates, the 'issue' and 'issuewild' are the relevant properties. For S/MIME Certificates the 'issuemail' is the relevant property. While the 'iodef' property is checked, no action is taken. A RRset may contain all the properties but only the properties relevant to the Certificate type affect the issuance decision.

The criteria below are used to establish whether to issue the Certificate.

A Certificate is not issued if:

- The RRset contains a critical unrecognized property tag.
- All instances of the relevant properties include an issuer-domain-name other than "pki.apple.com" or contain an empty string, or the property value exhibits malformed syntax.

A Certificate is issued if every Domain Name in the Certificate Application meet at least one of the conditions below:

- There is no Relevant RRset,
- For a TLS Certificate's FQDN, The 'issue' property lists the name "pki.apple.com",
- For a Wildcard Certificate's Wildcard Domain Name, the 'issuewild' property lists the name "pki.apple.com"
- For an S/MIME Certificate's Mailbox Address' domain-part, the 'issuemail' property for lists the name "pki.apple.com".

The CAA check is performed immediately before the issuance of the Certificate, but does not exclude the possibility of other CAA checks. See Section 4.2.1.

The Apple Public CA logs actions taken based on CAA records, and documents issuance prevented by CAA for feedback to the CAB Forum.

3.2.2.9. Mailbox Address Verification

Prior to issuing an S/MIME Certificate, the Apple Public CA verifies the Applicant controls the Mailbox Address by confirming either:

- The Domain Name contained in the domain portion of the Mailbox Address is owned or controlled by the Legal Entity in the Organization field in accordance with Section 3.2.2.4 of this CPS and Section 3.2.2.9.1 of the Apple Public CP, or,
- Receipt of a response utilizing the same Random Value previously sent by the Apple Public CA via email to the Mailbox Address being verified in accordance with Section 3.2.2.9.1 of the Apple Public CP. The Random Value is considered valid only for 24 hours from generation and if the response is received after expiration, the request for validation is resent with a new Random Value.

3.2.2.10.High Risk Certificate Requests

Prior to issuing a Certificate, every Base Domain Name in the request is compared to an externally compiled database of the top 1,000 most popular Domain

Names. If a Base Domain Name is present in the list, the request is considered high risk and it is rejected by default. An Applicant may be authorized for a domain on this list following manual review, in addition to all other validation checks

3.2.3. Authentication of Individual Identity

The Apple Public CA does not issue TLS Server Certificates to an Applicant who is a natural person.

The Apple Public CA does not issue S/MIME Certificates that include the name of a natural person.

3.2.4. Non-Verified Subscriber Information

The Apple Public CA does not include non-verified Subscriber information in Certificates.

3.2.5. Validation of Authority

Authority is validated based on Certificate type. When the Applicant is a Legal Entity, the Applicant Representative's authority to request Certificates on behalf of an organization is confirmed using information gathered during the Applicant's identity verification which relies on a Reliable Method of Communication as described in Section 3.2.21.

Root Certificate, Sub-CA Certificate and TLS Server Certificates

The Apple Public CA takes reasonable steps to establish that a Certificate Application is from Apple staff. Certificate Requesters authenticate to enrollment systems with the Identification Credential that verifies they are an employee of the Subscriber, i.e., Apple Inc., before a Certificate Application can be submitted.

For Root Certificate and Sub-CA Certificates, the Certificate Requestor is confirmed to be a Trusted Role and to have express authorization to submit a Certificate Application for these types of Certificates.

For TLS Server Certificates, a list of pre-approved Certificate Requesters, is included in the enrollment system limiting who can submit Certificate Applications.

S/MIME Certificates

For Mailbox-validated S/MIME Certificates, authority is implicit based on demonstration of control according to Section 3.2.2.9.

For Organization-validated S/MIME Certificates, authority of the request is verified through the demonstrated control by the Legal Entity over the Mailbox Address using a technical or administrative control.

3.2.6. Criteria for Interoperation

The Apple Public CA discloses Sub-CA certificates, including Cross-Certified Subordinate CA Certificates, in Appendix A - Apple Subordinate CAs Hierarchy.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-Key

Not applicable, since the Apple Public CA does not provide Certificate re-key as defined in Section 4.7.

3.3.2. Identification and Authentication for Re-Key After Revocation

Subscribers may request a new Certificate after a revocation. Those Certificate Applications follow the same process as the initial Certificate issuance.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

The Subscriber, or the Subscriber's representatives specified in Section 4.9.2, can request revocation. Those individuals are listed in the enrollment system; before they can request revocation, they must present their Identification Credential to access the enrollment system.

When a revocation is requested as result of a Certificate Problem Report, an RA Officer will request and/or execute revocation as discussed in Section 4.9.3. The RA Officer will identify to the enrollment system using appropriate credentials as discussed in Section 5.2.3.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

Root Certificate and Sub-CA Certificate

Only individuals in Trusted Roles working for the Apple Public CA may submit Certificate Applications for Root Certificates and Sub-CA Certificates.

TLS Server Certificates and S/MIME Certificates

Only the Applicant, an authorized Applicant Representative or an authorized Certificate Requester representing the Applicant may submit Certificate Applications. Those Certificate Applications may be submitted directly or through the use of automated agent (e.g., ACME client) that has been authorized by the Apple Public CA to access its enrollment system on behalf of the Applicant or its representatives.

The Apple Public CA will not issue TLS Server Certificates to an Applicant if either the Applicant, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Business is on any United States Government denied list, or other list that prohibits doing business with such organization.

4.1.2. Enrollment Process and Responsibilities

The Apple Public CA has an enrollment process that combines online and offline functions to obtain:

- An executed Subscriber Agreement or Terms of Use,
- Information about the Applicant including, but not limited to, organization name, contacts, and authorizing individuals,
- Information about the Certificate including, but not limited to, a CSR, Mailbox Address, and FQDNs,
- Appropriate approvals by authorized Applicant's representatives or the Applicants themselves.

Prior to issuing a Certificate, the Apple Public CA may collect evidence from sources other than the Applicant to confirm information to be included in the Certificate.

The Apple Public CA may leverage the verification information for an Applicant such as Legal existence, Address of Place of Business, Verified Method of Communication, Operational Existence, Domain Name, approver's name, title and authority for multiple Certificate Applications. The use of this information is limited to the maximum age specified in Section 4.2.1.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

The Apple Public CA verifies Certificate Application information using the practices in the sections noted next to each validation category.

During the validation process, to clarify any discrepancies, Validation Specialists are required to obtain additional information by contacting the Applicant, Applicant Representatives or other sources of information. When documentation is not available in English, the Apple Public CA will engage a translator.

Root Certificates and Sub-CA Certificates

- Applicant Identity: Sections 3.2.2.1, 3.2.2.2 and 3.2.2.3, and
- Identification and Authentication for each Trusted Role: Section 5.2.3.

TLS Server Certificates

- Applicant Identity: Sections 3.2.2.1, 3.2.2.2 and 3.2.2.3,
- Domain Ownership/Control: Section 3.2.2.4,
- Validation of Authority: Section 3.2.5,
- CAA: Section 3.2.2.8,
- High Risk Certificate Request: Section 3.2.2.10, and
- Wildcard Domain Validation: Section 3.2.2.6.

S/MIME Certificates

- Mailbox Address Verification: Section 3.2.2.9,
- Organization: Sections 3.2.2.1 and 3.2.2.3,
- Validation of Authority: Section 3.2.5,
- CAA: Section 3.2.2.8, and
- Domain Ownership/Control: Section 3.2.2.4.

Age of Validated Data

The Apple Public CA leverages information produced by a Certificate Application for approval of multiple Certificates. In order to use such information for a subsequent application, the date when the validation was performed is recorded, and the age of information is calculated to not exceed the limits below:

- Legal or operational existence and identity: 397 days

- Assumed name: 397 days

- Verified Method of Communication: 397 days
- Name, Title, Agency, and Authority: 397 days
- Domain Name for TLS and S/MIME Certificates: 397 days

4.2.2. Approval or Rejection of Certificate Applications

The Apple Public CA rejects Certificate Applications that cannot be verified based on the practices outlined in Section 4.2.1. for a specific Certificate type. Request rejection reasons may include, but are not limited to, requests that:

- are not for an Applicant's owned Domain Name,
- include Domain Names in the list of high risk Domain Names for which the Applicant is not the owner or has no control,
- include Internal Names or Reserved IP Addresses,
- include an Mailbox Address associated a Domain Name not owned/controlled by an authorized Applicant,
- are submitted by an Applicant representative without proper authority,
- remain incomplete or inconsistent after a reasonable amount of time after clarifications have been requested.

4.2.3. Time to Process Certificate Applications

Certificate Applications are processed within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in a relevant agreement.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions During Certificate Issuance

A Certificate is created and issued following approval of the Certificate Application.

Root Certificates and Sub-CA Certificates

The Apple Public CA generates CA Certificates during a scripted ceremony, conducted by trusted personnel observing separation of duties and two-person controls consistent with Section 5.2. Ceremonies for Root Certificates or Sub-CA Certificates, for Applicants other than Apple, are witnessed by external qualified auditors.

TLS Server Certificates and S/MIME Certificates

The Apple Public CA's enrollment system will use the information provided as part of the verification practices in Section 3.2, data in the online submission, and configuration constraints. Among other things, the system will:

- use the Public Key in the CSR,
- populate verified data in the Subject DN and prevent populating fields only with metadata such as ".", "-", and " " (i.e., space) characters,
- populate verified FQDNs and Wildcard Domain Names in the Subject Alternative Name extension that meet the Domain Label specifications in Section 7.1.4.4,
- perform automatic pre-issuance checks using both an internally-developed validator and a widely-distributed linting solution that verify, among other things, field limitations are respected, appropriate extensions are included, and field encodings are appropriate, and
- confirm that the Certificate has no missing or incorrect extensions and the Public Keys meet the parameters required in Section 6.1.6.

The Apple Public CA logs TLS Precertificates to Certificate Transparency logs to ensure the Certificate can operate with Apple and Google clients.

The Apple Public CA issues Certificates with a notBefore value that is no earlier than 24 hours of the actual signature date.

4.3.2. Notification To Subscriber by the CA of Issuance of Certificate

Upon issuance of a Certificate, the Apple Public CA may notify the Subscriber by sending an email to the Mailbox Address associated with the Certificate Application.

For Certificates that are requested via an automated agent, the notification email may not be sent but instead the agent may provide a notification that can be leveraged by the Subscriber system to notify the certificate holder.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

A Subscriber's use of the Certificate constitutes Certificate acceptance.

4.4.2. Publication of the Certificate by the CA

After issuance, Certificates are published to a private Repository, as specified in Section 2.1. The Apple Public CA also records issuance of TLS Server Certificates to Certificate Transparency logs.

The Apple Public CA publishes all Root Certificates and Sub-CA Certificate to the Repository.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

The Apple Public CA discloses in the CCADB all Sub-CA Certificates that chain up to Root Certificates trusted in Application Software Supplier programs.

For Sub-CA Certificates issued by a Root Certificate already trusted, disclosure occurs within 7 days of Sub-CA Certificate issuance and prior to issuance of any Certificates under such Sub-CA Certificate. For Sub-CA Certificates issued by a Root Certificate not yet included in Application Software Supplier programs, disclosure occurs when the Root Certificate is submitted to the programs.

The Apple Public CA notifies other entities by posting a TLS Server Certificate to multiple publicly accessible Certificate Transparency logs.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Certificate use must be consistent with the permitted uses described in Section 1.4.1.

Prior to using a Certificate, Subscribers represent that they will comply with the obligations outlined in Section 9.6.3. by accepting the Terms of Use or Subscriber Agreement.

4.5.2. Relying Party Public Key and Certificate Usage

Each Relying Party represents that prior to relying on a Certificate issued by the Apple Public CA, it will comply with the obligations outlined in Section 9.6.4.

Any warranties provided by the Apple Public CA are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the appropriate Relying Party Agreement set forth in the Repository.

4.6. CERTIFICATE RENEWAL

Certificate renewal is the issuance of a new Certificate to the Subscriber with the same Public Key and verified information (e.g. identity, domains, email address) in the Certificate. A renewed Certificate has a new serial number and an expiration date ending after the expiration date of the Certificate being renewed.

4.6.1. Circumstance for Certificate Renewal

No stipulation.

4.6.2. Who May Request Renewal

No stipulation.

4.6.3. Processing Certificate Renewal Requests

No stipulation.

4.6.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6. Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7. CERTIFICATE RE-KEY

Certificate re-key is the issuance of a new Certificate to the Subscriber with a new Public Key and same verified information (e.g. identity, domains, email address) in the Certificate. A re-keyed Certificate has a new serial number and same expiration date in the Certificate being re-keyed.

The Apple Public CA does not currently provide Certificate re-key.

4.7.1. Circumstance for Certificate Re-Key

No stipulation.

4.7.2. Who May Request Certification of a New Public Key

No stipulation.

4.7.3. Processing Certificate Re-Keying Requests

No stipulation.

4.7.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation.

4.7.6. Publication of the Re-Keyed Certificate by the CA

No stipulation.

4.7.1. Notification of Certificate Issuance by the CA to Other Entities.

No stipulation.

4.8. CERTIFICATE MODIFICATION

Certificate modification means the issuance of a new Certificate to the Subscriber with the same Public Key but different verified information (e.g. identity, domains, email) in the Certificate. A modified Certificate has a new serial number and same or other expiration date ending after the expiration date of the Certificate being modified.

The Apple Public CA does not currently provide Certificate modification.

4.8.1. Circumstance for Certificate Modification

No stipulation.

4.8.2. Who May Request Certificate Modification

No stipulation.

4.8.3. Processing Certificate Modification Requests

No stipulation.

4.8.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6. Publication of the Modified Certificate by the CA

No stipulation.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

The Apple Public CA provides revocation information for all Certificates and Precertificates issued by its Root Certificates and Sub-CA Certificates. Revocation for a Precertificate is available even when it was generated but no final Certificate was issued.

4.9.1. Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

A Subscriber may request revocation of its Certificate at any time for any reason.

TLS Server Certificates

The Apple Public CA will revoke a TLS Server Certificate within 24 hours after confirming one or more of the following occurred:

1. The Subscriber requests in writing, without specifying a reason, that the Apple Public CA revoke the TLS Server Certificate,
2. The Subscriber notifies the Apple Public CA that the original TLS Server Certificate Application was not authorized and does not retroactively grant authorization,
3. The Apple Public CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the TLS Server Certificate suffered a Key Compromise,
4. The Apple Public CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys),
5. The Apple Public CA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the TLS Server Certificate should not be relied upon, or
6. An Application Software Supplier asks to revoke a Subscriber's Certificate and all allowed appeal instances have been exhausted.

The Apple Public CA may revoke a TLS Server Certificate within 24 hours and will revoke a TLS Server Certificate within 5 days after confirming that one or more of the following occurred:

1. The TLS Server Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of this CPS,
2. The Apple Public CA obtains evidence that the TLS Server Certificate was misused,
3. The Apple Public CA confirms that a Subscriber has violated one or more of its material obligations under any relevant agreement,
4. The Apple Public CA confirms any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the TLS Server Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name),
5. The Apple Public CA confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN,
6. The Apple Public CA confirms a material change in the information contained in the TLS Server Certificate,

7. The Apple Public CA confirms that the TLS Server Certificate was not issued in accordance with the Apple Public Root CP or this CPS,
8. The Apple Public CA confirms that any of the information appearing in the TLS Server Certificate is inaccurate,
9. The Apple Public CA's right to issue TLS Server Certificates under the Apple Public Root CA expires or is revoked or terminated, unless the Apple Public CA has made arrangements to continue maintaining the CRL/OCSP Repository,
10. Revocation is required by the Apple Public Root CP and/or this CPS,
11. The Apple Public CA confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed,
12. The Private Key used by the Apple Public CA to issue the Certificate is suspected to have been compromised, or
13. The Apple Public CA is made aware of a violation of an Application Software Supplier's then-current program requirements and was not yet part of the Apple Public Root CP or this CPS, which resulted in the misissuance of the Certificate.

S/MIME Certificates

The Apple Public CA will revoke a S/MIME Certificate within 24 hours after confirming one or more of the following occurred:

1. The Subscriber requests in writing that the Apple Public CA revoke the Certificate,
2. The Subscriber indicates that the original Certificate Application was not authorized and does not retroactively grant authorization,
3. The Apple Public CA obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has been compromised or is suspected of compromise,
4. The Apple Public CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys), or
5. The CA obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon.

The Apple Public CA may revoke a Certificate within 24 hours and will revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6,
2. The Apple Public CA obtains reasonable evidence that the Certificate has been misused or used for a purpose outside of that indicated in the Certificate,
3. The Apple Public CA receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Terms of Use,
4. The Apple Public CA receives notice or otherwise becomes aware of any circumstance indicating that use of the Mailbox Address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted,
5. The Apple Public CA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate,
6. A determination that the Certificate was not issued in accordance with this CPS,
7. The Apple Public CA determines that any of the information appearing in the Certificate is inaccurate,
8. The Apple Public CA ceases operations for any reason, or its right to issue Certificates under the S/MIME Baseline Requirements expires or is revoked or terminated, and has not arranged for another CA to provide revocation support for the Certificate,
9. The Apple Public CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed,
10. The Apple Public CA Private Key used in issuing the Certificate is suspected to have been compromised,
11. Such additional revocation events as the Apple Public CA publishes in its policy documentation, or
12. The Apple Public CA is made aware of a violation of an Application Software Supplier's then-current program requirements and was not yet part of the Apple Public Root CP or this CPS, which resulted in the misissuance of the Certificate.

4.9.1.2. Reasons for Revoking a Sub-CA Certificate

The Apple Public CA will revoke a Sub-CA Certificate within 7 days after confirming one of the following occurred:

1. The APA requests revocation in writing,
2. The Apple Public CA becomes aware than the original request for the Sub-CA Certificate was not authorized and does not retroactively grant authorization,
3. The Private Key corresponding to the Public Key in the Sub-CA Certificate suffered a Key Compromise or no longer complies with the requirements of this CPS Sections 6.1.5 and 6.1.6,
4. The Apple Public CA obtains evidence that the Sub-CA Certificate was misused,
5. The Apple Public CA is made aware that the Sub-CA Certificate was not issued in accordance with the Apple Public Root CP, or this CPS,
6. The Apple Public CA determines that any of the information appearing in the Sub-CA Certificate is inaccurate or misleading,
7. The Apple Public CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate,
8. The Apple Public CA's right to issue Certificates under this CPS expires or is revoked or terminated, unless the Apple Public CA has made arrangements to continue maintaining the CRL/OCSP Repository, or
9. Revocation is required by the Apple Public Root CP, or this CPS.

4.9.2. Who Can Request Revocation

For S/MIME Certificates, the Subscriber who requested the original Certificate; or for TLS Server Certificates and Organization-validated S/MIME Certificates, an authorized Subscriber representative (i.e., Certificate Signer, Certificate Approver, Certificate Requestors) may request the revocation of the Certificate.

Application Software Suppliers, and other third parties may submit Certificate Problem Reports, as outlined in Section 1.5.2.1, informing the Apple Public CA of reasonable cause to revoke the Certificate.

The Apple Public CA reserves the right to revoke any Certificates, without notice, for any reason, or if it believes the Private Key has been compromised.

4.9.3. Procedure for Revocation Request

The Apple Public CA provides an online revocation process available 24x7 to Subscribers. The Subscriber, or Subscriber representative, will be required to authenticate to the enrollment system with their Identification Credential. After authentication, the requestor requests revocation of their Certificate, selects the

most appropriate revocation reason, and then the Certificate will be automatically revoked. After the Certificate is revoked, a revocation notification is sent to the Subscriber.

The Apple Public CA provides instructions on how to submit a Certificate Problem Report publicly available online 24x7. After a Certificate Problem Report is received for a Certificate issued by Apple Public CA under this CPS, it will be investigated by the Apple Public CA compliance team within 24 hours of receipt. If, as a consequence of the investigation, revocation is required for a TLS or S/MIME Certificate, an Apple Public CA representative will authorize the revocation in accordance with Section 4.9.1.1. and an RA Officer will execute it.

If a revocation is required for a Sub-CA Certificate, the Compliance team will engage the APA for revocation approval and a ceremony will be promptly scheduled. After a Sub-CA Certificate is revoked, the Apple Public CA reports such revocation to Application Software Suppliers through the CCADB within 30 days of revocation. If the revocation is due to a security concern, the Apple Public CA will file an appropriate public disclosure with the Application Software Suppliers that require it (e.g. Mozilla).

4.9.4. Revocation Request Grace Period

There is no grace period within which the Subscriber must make a revocation request. Revocations can only be processed for Certificates that have not expired.

4.9.5. Time Within Which CA Must Process the Revocation Request

A revocation request submitted to the online enrollment system is processed immediately.

For revocation requests submitted through a Certificate Problem Report, a preliminary report is provided to the party that submitted the Certificate Problem Report and to the Subscriber associated to the Certificate. Reports to the Subscriber are submitted to the email address associated to the original Certificate Application.

The Apple Public CA processes revocation requests within the timeframes outlined in Section 4.9.1.1.

4.9.6. Revocation Checking Requirement for Relying Parties

Relying Parties are solely responsible for performing revocation checking on all Certificates in the chain before deciding whether or not to rely on the information in a Certificate. The Apple Public CA provides revocation status via mechanisms that are embedded in the Certificate (e.g., CRL Distribution Point or OCSP URI).

4.9.7. CRL Issuance Frequency

For the status of Subscriber Certificates, the Apple Public CA issues a new CRL (i.e., thisUpdate) at least once every twenty-four (24) hours. CRLs are issued with a nextUpdate time no longer than 7 days from the thisUpdate time.

For the status of Sub-CA Certificates, the Apple Public CA issues a new CRL at least once every twelve (12) months. CRLs are issued with a nextUpdate time at most twelve (12) months from the thisUpdate time. When a Sub-CA Certificate is revoked, a new CRL will be generated within 24 hours.

Within twenty-four (24) hours of issuing its first Certificate from a new sub-CA, the Apple Public CA generates and publishes a CRL (complete or partitioned). Afterwards, CRLs are continuously issued until all Sub-CAs associated to the Public Key used to sign the CRL are expired or revoked.

The Apple Public CA makes CRLs publicly-accessible via an HTTP URL, which is disclosed in the Certificate itself as shown in profiles in Section 7.1.2.11.2.

4.9.8. Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation.

4.9.9. On-Line Revocation/Status Checking Availability

The Apple Public CA's OCSP implementation conforms to RFC 6960 and RFC 8954.

The Apple Public CA provides OCSP status using a delegated OCSP model. Certificates used to sign OCSP responses contain the id-pkix-ocsp-nocheck extension.

The appropriate OCSP Responder is available via the URI noted in the Authority Information Access extension in the Certificate.

The Apple Public CA provides URLs for all CRLs signed by its Sub-CA Certificates to Application Software Suppliers that require them, in an appropriately-formatted structure (e.g., JSON Array), before any Subscriber Certificates are issued. URL publication to the CCADB is carried out in accordance with Mozilla Root Store Policy Section 4.1 and the Apple Root Certificate Program.

4.9.10.On-Line Revocation Checking Requirements

Before relying on a Certificate, a Relying Party must confirm the validity of a Certificate in accordance with Section 4.9.6.

The Apple Public CA's OCSP service supports the HTTP GET method for receiving requests. A valid OCSP status request 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.

Apple Public CA's OCSP service supports the use of the Nonces extension (1.3.6.1.5.5.7.48.1.2) when present in the request.

For status of Subscriber Certificates, the OCSP responses will have a validity interval between eight (8) hours and ten (10) days. For responses shorter than 16 hours, updates are available prior to one-half of the validity period before the nextUpdate. For responses equal or greater than 16 hours, updates are available at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For status of Sub-CA Certificates, the OCSP responses will have a validity interval no larger than 210 days. When a Sub-CA Certificate is revoked, a new response will be available within 24 hours.

Appropriate response values are provided in Section 7.3.1.

4.9.11. Other Forms of Revocation Advertisements Available

No other forms of revocation advertisements are available.

4.9.12. Special Requirements re Key Compromise

In the event of key compromise of the a Root or Sub-CA Private Key, the Apple Public CA will use the practice in Section 5.7.3.

In the event that a Subscriber's Private Key is reported as comprised by a party other than the Subscriber, the Apple Public CA will request that this party proves possession of the Private Key by either submitting it via email, as part of the Certificate Problem Report; or, by signing a randomly generated string provided by the Apple Public CA as a follow up to the initial report. If possession is proved, the Apple Public CA will revoke all instances of that key across all Subscribers.

If the Subscriber requests that the Apple Public CA revoke the Certificate with the keyCompromise reason, and has not previously demonstrated and cannot currently demonstrate possession of the associated Private Key of that Certificate, the Apple Public CA will revoke all Certificates associated with that Subscriber that contain that Public Key on the basis of the Subscriber Representative's access to the enrollment system needed to submit the request. The Apple Public CA prevents issuance of future Certificates with the keys that have been revoked.

When the Apple Public CA obtains verifiable evidence of Private Key compromise for a previously-revoked Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, the Apple Public CA will update the CRL entry to enter keyCompromise as the reason in the reasonCode extension and the revocation date when it is determined that the Private Key of the Certificate was compromised prior to the revocation date that is indicated in the CRL entry for that Certificate.

Note: Backdating the revocationDate field is an exception to best practice described in RFC 5280 (section 5.3.2); however, the Mozilla Root Store Policy specifies the use of the revocationDate field to support TLS implementations that process the revocationDate field as the date when the Certificate is first considered to be compromised.

4.9.13. Circumstances for Suspension

The Apple Public CA does not support Certificate suspension.

4.9.14. Who Can Request Suspension

No stipulation.

4.9.15. Procedure for Suspension Request

No stipulation.

4.9.16. Limits on Suspension Period

No stipulation.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

The Apple Public CA offers Certificate status information using CRLs and OCSP Responses. Certificate status services are available via the CRL Distribution Point or the OCSP pointer noted in the Certificates.

Revocation entries on a CRL or OCSP Response are available until after the expiration date of the revoked Certificate.

4.10.2. Service Availability

The Apple Public CA takes commercially reasonable steps to provide Certificate status services 24x7. Those services are operated with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

The Apple Public CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3. Operational Features

No stipulation.

4.11. END OF SUBSCRIPTION

A Subscriber may end subscription for a Certificate by allowing the Certificate to expire, or by revoking the Certificate prior to expiration.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy and Practices

The Apple Public CA, when authorized by the Subscriber, maintains a copy of the Subscriber Private Keys associated with S/MIME Certificates used for email

encryption. Those Private Keys are escrowed in an encrypted format, which provides a strength commensurate to the Private Key being escrowed.

Escrowed keys can only be recovered after confirming the authority of the party requesting the Private Key. Subscribers must present their Identification Credential to the enrollment system before they can recover Private Keys. Apple representatives may obtain an escrowed Private Key after they demonstrate they have been authorized by the Apple's legal or human resources teams to request the recovery.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

The Apple Public CA implements management, operational and physical controls as specified in Section 5 of the Apple Public Root CP.

5.1. PHYSICAL SECURITY CONTROLS

5.1.1. Site Location and Construction

Equipment supporting CA operations resides within a physically secured location in geographically separated Apple owned or controlled facilities.

5.1.2. Physical Access

Physical protection is achieved through the creation of clearly defined security perimeters with appropriate physical barriers to entry around the business premises, data center, and CA operations.

Data center site physical security mechanisms include facility design and construction, perimeter security (e.g., heavy duty fences, gates, and barriers), and logical and personnel controls (e.g., access management, badging, and multi-factor authentication).

Within the data center, additional security controls are placed on the High Security Environments ("HSE") housing CA operations. Separate logical and physical security mechanisms protect the HSEs, situated in either cages or secured rooms, and include access management controls, such as two-person access and multi-factor authentication.

By default, access to the CA operations room or cage is disabled for all personnel, with access provisioning granted on an as-needed basis for specific time intervals. Access to safes protecting assets requires two-person control.

Apple's global security team is responsible for physical access to Apple data centers and HSEs, including access management systems, access records, monitoring and alerting systems, and security personnel to provide a continuous presence at each data center facility.

5.1.3. Power and Air Conditioning

Equipment is protected to reduce risks from power and air conditioning disruption or failure. Power is maintained in emergency situations by uninterrupted power supplies and generators. Redundant power supplies are tested on a regular basis.

5.1.4. Water Exposures

Equipment is protected to reduce risks from water exposure by means of temperature and humidity monitoring.

5.1.5. Fire Prevention and Protection

The data centers are protected with fire suppression systems, alarms, and monitors.

5.1.6. Media Storage

Media is maintained securely within the CA facilities and is subject to the same degree of protection as the CA hardware. Backups are stored at secondary data center locations, as per Section 5.1.8.

5.1.7. Waste Disposal

Media used to collect sensitive information is destroyed or zeroized prior to disposal.

Cryptographic devices are physically destroyed or zeroized in accordance with manufacturer's guidance prior to disposal.

5.1.8. Off-Site Backup

Backups are taken at regular intervals and stored at alternate locations as described in Section 5.4.5. For purposes of backup and recovery, offline Root and Sub-CA Private Keys, which are stored in encrypted form, are transported to alternate secure storage under dual control. The backups exist in multiple copies in different geographic locations.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

Individuals in Trusted Roles have access to or control over cryptographic operations, including access to restricted operations within the Apple Public CA. Individuals in Trusted Roles must be Apple employees whose identity has been confirmed through background checking procedures as defined in Section 5.3 and who have accepted the responsibilities of a Trusted Role. Functions performed by persons in Trusted Roles are distributed in such a manner that prevents one person from subverting the security and trustworthiness of CA operations.

The responsibilities for each of the Trusted Roles include administration and operation tasks as described in the sections below.

5.2.1.1. CA Administrator

The CA Administrator is responsible for installation, configuration, and maintenance of the CA software, configuring Certificate Profiles, and generating and backing up Root and Sub-CA keys. CA Administrators do not issue Certificates to Subscribers.

5.2.1.2. RA Officer

The RA Officer, also known as a Validation Specialist, is responsible for verifying the identity of Applicant / Subscribers and accuracy of information included in Certificates, approving and executing the issuance of Certificates, and requesting the revocation of Certificates.

5.2.1.3. Audit Administrator

The Audit Administrator is responsible for reviewing, maintaining, and archiving audit artifacts and performing or overseeing internal compliance audits to ensure that the CA and other systems are operating in accordance with this CPS.

5.2.1.4. Operator

Operators, such as system administrators and CA operators, are responsible for keeping systems updated with software patches, hardware upgrades, and other maintenance needed for system stability and recoverability.

5.2.1.5. RA Administrator

RA Administrators install, configure and manage the RA software, including Sub-CAs and Certificate Profiles.

5.2.2. Number of Persons Required per Task

Root and Sub-CA Private Keys are backed up, stored, and recovered by individuals in Trusted Roles (both CA Administrators) under multi-person control in a physically secured environment.

Contractors serving in Trusted Roles will perform their functions under the supervision of a second Trusted Role individual who is an Apple employee.

5.2.3. Identification and Authentication for Each Role

Individuals in Trusted Roles identify and authenticate themselves using multi-factor authentication, including a certificate-based credential, before being allowed access to the systems necessary to perform their Trusted Roles.

The Apple Public CA temporarily locks access to secure CA processes if more than 5 consecutive login attempts fail.

5.2.4. Roles Requiring Separation of Duties

To accomplish separation of duties, Apple Public CA specifically designates individuals to the Trusted Roles defined in Section 5.2.1 above. Audit Administrators and RA Officers may not concurrently hold any other Trusted Role.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

Individuals in Trusted Roles are Apple personnel who have successfully completed a background check consistent with federal, state, and local regulations and have demonstrated the trustworthiness, skills and experience to accept Trusted Role responsibilities. Personnel in Trusted Roles undergo training prior to performing any duties as part of that role.

5.3.2. Background Check Procedures

Apple implements several processes at both time of hire and throughout an employee's tenure to assess and validate an individual's identity and trustworthiness.

5.3.2.1. Identity verification

Apple employees complete identity verification at time of hire. U.S. based Apple employees successfully complete the verification by means of government-issued photo identification compliant with the requirements of the U.S. Department of Homeland Security Form I-9 Employment Eligibility Verification.

5.3.2.1. Trustworthiness assessment

Apple employees are required to successfully complete a background check at time of hire. Background checks can include both criminal and non-criminal services (i.e. education verification and previous employment verification) consistent with federal, state, and local regulations.

Every Apple employee's performance is reviewed on a yearly basis to ensure they are meeting Apple's high standards.

5.3.3. Training Requirements and Procedures

Individuals serving as RA Officers, also known as Validation Specialists, that perform information verification duties, receive skills-training and pass an examination prior to commencing their job role. This training includes:

- Basic Public Key Infrastructure knowledge,
- Authentication and vetting policies and procedures,
- Common threats to the information verification process (including phishing and other social engineering tactics),
- Applicable functions relative to their assigned Trusted Role.

The Apple Public CA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a satisfactory skill level.

5.3.4. Retraining Frequency and Requirements

Apple employees complete training at time of hire and on an ongoing basis. Annual training includes but is not limited to: Worldwide Business Conduct, Privacy, and Compliance and Security training, with required modules determined by role and access level.

Individuals serving as RA Officers are expected to maintain skill levels consistent with the requirements of Section 5.3.3 and are retrained as requirements and responsibilities are added or modified.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7. Independent Contractor Requirements

Contractors are allowed to serve in Trusted Roles described in Sections 5.2.1.2 and 5.2.1.4. Contractors are subject to training practices described in Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

5.3.8. Documentation Supplied to Personnel

Policies and procedures are posted in an internal site that is made available to individuals in Trusted Roles.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

The Apple Public CA configures its Certificate Systems, Certificate Management Systems, and Root CA Systems to record essential security events. When specific events cannot be logged automatically, manual procedures are put in place to record the event.

The Apple Public CA records the following events:

1. CA certificate and key lifecycle events, including:
    i. Key generation, backup, storage, recovery, archival, and destruction,
    ii. Request of Certificate issuance, renewal, modification, re-key, and revocation,
    iii. Approval and rejection of certificate requests above in Section 5.4.1 (1)(ii),
    iv. Cryptographic device lifecycle management events,
    v. Generation of Certificate Revocation Lists,
    vi. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10), and
    vii. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    i. Request of Certificate issuance, renewal, modification, re-key, and revocation,

ii. All verification activities stipulated this CPS,

iii. Approval and rejection of certificate requests above in Section 5.4.1 (2)(i),

iv. Issuance of Certificates,

v. Generation of Certificate Revocation Lists, and

vi. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).

3. Security events, including:

i. Successful and unsuccessful PKI system access attempts,

ii. PKI and security system actions performed,

iii. Security profile changes,

iv. Installation, update and removal of software on a Certificate System,

v. System crashes, hardware failures, and other anomalies,

vi. Firewall and router activities, and

vii. Entries to and exits from the CA facility.

For each event, the Apple Public CA records the date and time, type of event, and user or system that caused the event or initiated the action.

The Apple Public CA makes these records available to its external auditor as proof of compliance with this CPS.

5.4.2. Frequency of Processing and Archiving Audit Logs

The Apple Public CA reviews system logs at least monthly to detect anomalies or irregularities. Automated tools are used to alert for specific conditions. Reviewed activities are tracked and documented, and are made available to external auditors upon request.

5.4.3. Retention Period for Audit Logs

Audit logs are retained for a minimum of two (2) years after the following:

1. For CA certificate and key lifecycle management event records (specified in Section 5.4.1(1)), after the later occurrence of:

i. the destruction of the CA Private Key, or

ii. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key,

2. For Subscriber Certificate lifecycle management event records (specified in Section 5.4.1(2)), after the expiration of the Subscriber Certificate,

3. For security event records (as specified in Section 5.4.1(3)) after the event occurred.

Apple Public CA makes these audit logs available to its external auditor upon request.

5.4.4. Protection of Audit Log

Online audit logs are maintained securely within the CA facilities and are subject to the same degree of protection as the CA hardware. Archived audit logs are maintained in a secondary storage location as per Section 5.4.5. CA system configurations and operational procedures ensure that only authorized personnel may read or archive audit logs, and that audit logs are protected from unauthorized modification or deletion.

5.4.5. Audit Log Backup Procedures

Systems hosting audit data are backed up daily, The data is replicated to a secondary site, which is in a geographically separated Apple facility. Audit logs are archived monthly and retained for the duration of the retention period described in Section 5.4.3.

5.4.6. Audit Collection System (Internal Vs. External)

Audit logs are collected using enterprise-grade storage management systems, stored only within Apple data centers, as defined in Section 5.4.5.

5.4.7. Notification To Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

The Apple Public CA performs an annual risk assessment to:

1. Identify threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes,

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes, and

3. Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.5. RECORDS ARCHIVAL

5.5.1. Types of Records Archived

The Apple Public CA archives the following types of records:

1. Records of the events listed in Section 5.4.1,

2. Known and suspected violations of physical security and, if applicable, remedial actions taken as a result,

3. All versions of the Apple Public Root CP and this CPS,
4. Agreements (e.g., Relying Party Agreement, Subscriber Agreement, Terms of Use),
5. System and equipment configurations, modifications, and updates,
6. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2,
7. Issued Certificates,
8. Data and applications necessary to verify the archive contents,
9. Compliance auditor reports,
10. Changes to audit parameters,
11. Attempts to delete or modify audit logs,
12. Access to Private Keys for key recovery purposes (S/MIME Certificates only),
13. Export of Private Keys,
14. Appointment of an individual to a Trusted Role,
15. Destruction of a cryptographic module,
16. All Certificate compromise notification requests,
17. Certificate Problem Reports,
18. Remedial action taken as a result of violations of physical security, and
19. Violations of this CPS.

5.5.2. Retention Period for Archive

Records listed in Section 5.5.1 above are retained for at least two (2) years after any Certificate ceases to be valid or as long as they are required to be retained per Section 5.4.3, whichever is longer.

Apple Public CA also retains archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates after the later occurrence of:

- such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
- the expiration of all the Subscriber Certificates relying upon such records and documentation

5.5.3. Protection of Archive

Archive records are maintained in a manner to prevent unauthorized modification, substitution, or destruction.

The systems hosting the archived data therein are subject to authentication and authorization mechanisms, redundancy, backup storage in secondary sites, equipment updates and media refreshes.

Apple ensures that the archived records are retained in the software systems until no longer needed, or migrated to a replacement system in the event that the record retention requirement is longer than the lifespan of the software system.

5.5.4. Archive Backup Procedures

The Apple Public CA archives are backed up to storage in a different, geographically separated, Apple owned or controlled facility or service.

5.5.5. Requirements for Time-Stamping of Records

The systems hosting the archived data automatically timestamp archive records as they are created. System time is synchronized using the Network Time Protocol (NTP). Cryptographic time-stamping of archive records is not performed.

5.5.6. Archive Collection System (Internal or External)

The Apple Public CA collects archive information internally.

5.5.7. Procedures to Obtain and Verify Archive Information

Apple restricts access to archive data to authorized trusted personnel and Apple staff only, in accordance with internal procedures and security policies. Apple does not release any archived information except as allowed by law as specified in Section 9.

5.6. KEY CHANGEOVER

Towards the end of each Root CA or Sub-CA lifetime, a new CA Key Pair is generated following the procedures in Section 6.1.1.1.

The old Root CA Private Key will no longer be used to sign new Sub-CA Certificates. All subsequently issued Sub-CA Certificates issued from the new Root CA are signed with the new Private Key

The old Sub-CA Private Key will no longer be used to sign new Subscriber Certificates, but will be used to sign CRLs and delegated OCSP Responder Certificates. All subsequently issued Subscriber Certificates, CRLs, and delegated OCSP Responder Certificates issued from the new Sub-CA are signed with the new Private Key.

The Apple Public CA will continue to protect its old Private Keys, and makes the old Root and Sub-CA Certificates available to verify signatures at least until all of the Certificates signed with the respective Private Key have expired.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

The Apple Public CA maintains an Incident Response Plan and a Disaster Recovery Plan as specified in Section 5.7.1 of the Apple Public Root CP.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

In the event of a disaster in which computing resources, software, and/or data is corrupted, appropriate escalation, incident investigation, and response will be initiated. The Apple Public CA will halt the issuance or validation of Certificates if compromise of those systems, or data, may cause the generation of Certificates or status responses that do not comply with this CPS.

In the event of a disruption, when restoring operations, the Apple Public CA will give priority to reestablishing the generation of Certificate status information.

5.7.3. Entity Private Key Compromise Procedures

In the event of compromise, suspected compromise, or loss of a Root or Sub-CA Private Key, appropriate escalation, incident investigation, and response will be initiated. This response will include filing an incident report with the Application Software Suppliers as stated in Section 5.7.1 of the Apple Public Root CP.

If the investigation confirms the need for revocation of a Sub-CA Certificate, the Apple Public CA will revoke the compromised Certificate. Subsequently, a new CA Key Pair will be created, and a new Sub-CA Certificate created. The Apple Public CA will also revoke, and if necessary reissue, all impacted Subscriber Certificates.

If a Root Certificate is compromised, the Apple Public CA will work with Application Software Suppliers to address the retirement of the Certificate in an orderly manner. Actions prior to retirement may include the revocation of all Sub-CA and Subscriber Certificates and subsequent re-issuance.

5.7.4. Business Continuity Capabilities After a Disaster

The Disaster Recovery Plan noted in Section 5.7.1 relies on preparation before a disaster event as well as actions triggered by the disaster event.

Prior to a disaster event, systems are required to be architected with multiple redundant layers and are allocated in multiple geographically diverse locations to provide continuous operation. Risk vectors are re-evaluated continuously and the plan is strengthened based on findings.

When a disaster impacts one of the redundant layers, the other layers will continue operations without, or with minimal, interruption.

5.8. CA OR RA TERMINATION

Any decision to terminate the Apple Public CA shall be approved by the Apple CA Policy Authority prior to the effective date of termination.

As part of the termination procedure, the Apple Public CA will execute the termination plan that addresses the following:

- Provision of notice to parties affected by the termination,
- The revocation of Certificates issued by the Apple Public CA,
- The preservation of the Apple Public CA's archives and records.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

6.1.1.1. CA Key Pair Generation

The Apple Public CA generates CA Key Pairs used in Root and Sub-CA Certificates during a scripted ceremony, conducted by trusted personnel observing separation of duties and two-person controls consistent with Section 5.2, witnessed by external qualified auditors. A report is produced by the auditors opining on the ceremony.

Ceremonies are conducted in secure facilities described in Section 5.1. CA Key Pairs are generated using FIPS-validated Cryptographic Modules complying with Section 6.2.1. The ceremony produces evidence available to auditors to verify that appropriate controls were met.

6.1.1.2. RA Key Pair Generation

No stipulation.

6.1.1.3. Subscriber Key Pair Generation

The Apple Public CA does not generate Key Pairs for TLS Server Certificates. These Key Pairs are generated by the Subscriber. Apple Public CA may generate Key Pairs when Apple Public CA is the Subscriber.

Before including a Subscriber's key in a Certificate, the key is verified to meet the minimum sizes specified in Section 6.1.5, parameters in Section 6.1.6, and checked against weak keys (e.g., Debian weak keys). Keys that do not meet those specifications result in their associated Certificate Application being rejected.

The Apple Public CA does not generate Key Pairs used in S/MIME Certificates except when those keys are used in Certificates issued to Apple staff. All keys are verified to meet size requirements in Section 6.1.5 and parameters in Section 6.1.6.

The Apple Public CA prevents known compromised keys associated with revoked Certificates or rejected Certificate Applications to be used in a new Certificate Application.

The Apple Public CA also uses a validation mechanism prior to issuing the Certificate. This mechanism includes evaluation of the submitted Public Key using constraints configured as a result of monitoring guidelines and warnings from CAB Forum, Application Software Supplier websites, NIST and other relevant sources. These constraints include detecting keys generated with known flawed methods, or that are associated with demonstrated or proven methods that

expose the Applicant's Private Key to compromise. Keys generated with those methods are rejected.

6.1.2. Private Key Delivery to Subscriber

For S/MIME Certificates issued to Apple staff, the Key Pair is provided to the Subscriber using a PKCS#12 file protected by a password. The strength of the protection provided by the PKCS#12 and password is at least 128 bits. The PKCS#12 file is distributed separately from the password.

6.1.3. Public Key Delivery to Certificate Issuer

Public Keys for TLS Server Certificates are submitted using a PKCS#10 CSR over a TLS connection.

6.1.4. CA Public Key Delivery to Relying Parties

Root Certificates are distributed via Application Software Suppliers' operating systems, browser, mail and other clients. Root Certificates are also hosted on the online Repository indicated in Section 2.1.

Sub-CA Certificates are hosted online and can be reached through a URL provided in the Authority Information Access' calssuer field of the Subscriber Certificate. Software clients used by Relying Parties can leverage path discovery to obtain Certificates using the calssuer information.

6.1.5. Key Sizes

6.1.5.1. Root Certificates

The Apple Public CA generates CA Key Pairs for its Root Certificates and ensures they meet the following:

- RSA Modulus Size (bits): 4096
- Elliptic Curve: NIST P-384

6.1.5.2. Sub-CA Certificates

The Apple Public CA generates CA Key Pairs for its Sub-CA Certificates and ensures they meet the following:

- RSA Modulus Size (bits): 2048, 3072 or 4096
- Elliptic Curve: NIST P-256 or P-384

6.1.5.3. Subscriber and OCSP Responder Certificates

The Apple Public CA ensures that Key Pairs used in Subscriber and OCSP Responder Certificates meet the following:

TLS Server Certificates:

- RSA Modulus Size (bits): 2048, 3072 or 4096
- Elliptic Curve: NIST P-256 or P-384

S/MIME Certificates:

- RSA Modulus Size (bits): 2048, 3072 or 4096
- Elliptic Curve: NIST P-256 and P-384

OCSP Responder Certificates:

- RSA Modulus Size (bits): 2048, 3072 or 4096
- Elliptic Curve: NIST P-256 or P-384

6.1.6. Public Key Parameters Generation and Quality Checking

For Subscriber RSA keys, the enrollment system confirms that the value of the public exponent is an odd number in the range between $2^{16} + 1$ and $2^{256} - 1$. The system also confirms the modulus is an odd number, not the power of a prime, and has no factors smaller than 752.

For Subscriber ECDSA keys, the enrollment system confirms the validity of all keys using the ECC Partial Public Key Validation Routine first two checks.

For CA RSA keys, the CA system confirms that the value of the public exponent is an odd number in the range between $2^{16} + 1$ and $2^{256} - 1$. The system also confirms the modulus is an odd number, not the power of a prime, and has no factors smaller than 752.

For CA ECDSA keys, the CA system confirms the validity of all keys using the ECC Partial Public Key Validation Routine first two checks.

6.1.7. Key Usage Purposes (as per X.509 v3. Key Usage Field)

The Apple Public CA uses the Private Keys corresponding to Root Certificates only for purposes of signing:

- The Root Certificate itself,
- Sub-CA Certificates,
- Certificates for OCSP Responders, and,
- CRLs.

The use of a specific key is determined by the Key Usage and Extended Key Usage extensions in the X.509 Certificate. The Apple Public CA uses in its Certificates only the Key Usage and Extended Key Usage extension values defined in Section 7.2.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

Root, Sub-CA, and OCSP Responder Private Keys are generated and stored in Cryptographic Modules that are validated as FIPS 140-2 level 3.

6.2.2. Private Key (n out of m) Multi-Person Control

The Apple Public CA generates Root CA and Sub-CA Key Pairs, including backups, and activates Private Keys for signature operations in a physically secure environment, under multi-person control by individuals in Trusted Roles.

6.2.3. Private Key Escrow

Root and Sub-CA Private Keys are backed up but not escrowed.

S/MIME Private Keys may be escrowed in accordance with practices in Section 4.12.

6.2.4. Private Key Backup

The Apple Public CA backs up its Root CA and Sub-CA Private Keys in a physically secure environment, under multi-person control by individuals in Trusted Roles, storing at least one backup at a secure, secondary location. All copies of its Root and Sub-CA Private Keys are protected in the same manner as the original.

6.2.5. Private Key Archival

The Apple Public CA does not archive Private Keys used in Root Certificates or Sub-CA Certificates.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

Transfer of the Root and Sub-CA Private Key into or from a Cryptographic Module, performed only for key backup procedures, is done in accordance with the manufacturers' guidelines, under multi-person control by individuals in Trusted Roles. The Apple Public CA never allows the Private Keys to exist in plaintext outside of these Cryptographic Modules at any point in time.

6.2.7. Private Key Storage on Cryptographic Module

Root and Sub-CA Private Keys, including backups, are stored in Cryptographic Modules that meet the specifications in Section 6.2.1.

6.2.8. Method of Activating Private Key

Activation of Root and Sub-CA Private Keys is done in accordance with the guidelines provided by the manufacturer of the Cryptographic Module, under multi-person control, performed by individuals in Trusted Roles. Activation data will be protected from disclosure or communication to any external party.

6.2.9. Method of Deactivating Private Key

Sub-CA Private Keys are deactivated upon executing a deactivation command. Root Private Keys are deactivated upon system power off. The Apple Public CA prevents unauthorized access to any activated Cryptographic Modules.

6.2.10. Method of Destroying Private Key

Root and Sub-CA Private Keys on Cryptographic Modules will be destroyed by individuals in Trusted Roles in accordance with instructions and documentation provided by the manufacturer, when no longer needed.

6.2.11. Cryptographic Module Rating

See specification in Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

Public Keys are archived as part of the Certificate archival in compliance with Section 5.5.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The operational period for Key Pairs is the same as the Validity Period for associated Certificates.

Certificates issued by the Apple Public CA are limited to the following Validity Periods:

- Root Certificates: up to 7390 days.
- Sub-CA Certificates: up to 3740 days.
- TLS Server Certificates: up to 396 days.
- S/MIME Certificates: up to 824 days.
- OCSP Responder for Root: up to 180 days.
- OCSP Responder for Sub-CA: up to 90 days.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

The Apple Public CA follows the manufacturer specifications for the activation data required for Root and Sub-CA Private Keys. As specified in Section 6.2.2, to activate a Cryptographic Module, M of N secrets are required. Those secrets are generated when the Cryptographic Module is initialized and they are stored on separate secure tokens.

6.4.2. Activation Data Protection

The Apple Public CA protects from disclosure the data used to unlock Private Keys using a combination of cryptographic and physical access control mechanisms. Secure tokens with activation data are kept under multi-person control, as specified in Section 5.1.2, and require a PIN of minimum eight (8) digits to unlock for use.

The Apple Public CA locks access to secure CA processes if a certain number of failed password attempts occur as specified in Section 5.2.3.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

The Apple Public CA configures systems to meet the following security technical requirements, at a minimum:

- User identities are authenticated before access is permitted to systems or applications,
- User privileges are managed to limit users to their assigned roles,
- Audit records are generated and archived for applicable transactions,
- Domain integrity boundaries are enforced for security critical processes, and
- Recovery is supported for key or system failures.

The Apple Public CA enforces multi-factor authentication on any account capable of directly causing Certificate issuance.

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

The Apple Public CA acquires CA and OCSP Responder software from a reputable third-party. The vendor has an established software development life-cycle management process.

The Apple Public CA develops some software modules in-house, also following an established software development life-cycle management process.

For Apple Public CA operations, this software is installed on dedicated hardware.

Purchases of hardware and software assets are conducted using established procurement processes and delivered using tracked and verifiable mechanisms in order to reduce the likelihood of tampering

The Apple Public CA uses a formal configuration management methodology for installation and ongoing maintenance of any CA system. Any modifications or upgrades to the system are documented and controlled.

6.6.2. Security Management Controls

The Apple Public CA system configurations are periodically reviewed to identify any unauthorized changes.

The Apple Public CA maintains change control mechanisms to document, control, monitor, and maintain the installation and configuration of the CA systems, including any modifications or upgrades. When loading software onto a CA system, the Apple Public CA verifies that the software is the correct version and is supplied by the vendor free of any modifications.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

Network security measures are in place to protect against denial of service and intrusion attacks, including denying all but the necessary services to support the CA systems, network segmentation, access limited to CA personnel, and regular review of network, firewall, ACL, and load balancer configurations. Initial configurations are reviewed to verify that all versions are correct and are set as supplied by the vendor free of any modifications.

6.8. TIME-STAMPING

Apple Public CA systems are continuously synchronized using the Network Time Protocol ("NTP") by means of NTP pools dedicated to each Apple data center. NTP services on CA systems are monitored to ensure the NTP service is running and to detect if the system clock is out of synchronization with UTC.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

The CA System generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1. Version Numbers

Certificates issued under this CPS are X.509 version 3.

7.1.2. Certificate Content and Extensions

The Apple Public CA issues Certificates with the content and extensions shown in the following sections. All extensions are set in accordance with RFC 5280.

For Certificates other than Root Certificates, the Apple Public CA may include private Certificate extensions as long as they are: 1) marked non-critical, and 2) identified by an OID within an arc owned by the Subscriber (i.e., Apple Inc. or a subsidiary).

7.1.2.1. Root CA Certificate Profile

The Apple Public CA issues Root Certificates that are limited to issuance of only one type of Certificate (i.e., TLS Server Certificates or S/MIME Certificates). This dedicated use is reflected in the Common Name.

Field	Description
tbsCertificate	-
version	v3(2)
serialNumber	A non-sequential number of 128 bits containing at least 64 bits of output from a CSPRNG.
signature	A signature algorithm specified in Section 7.1.3.2.
issuer	Encoded value is byte-for-byte identical to the encoded subject
validity	notBefore: the value of the certificate signing operation notAfter: a value not to exceed what is specified in Section 6.3.2.
subject	Encoding, length and order is specified in Section 7.1.4.2. Common Name structure is specified in Section 7.1.2.10.2. - Country, - Organization, and - Common Name.
subjectPublicKeyInfo	A key type, size and encoding specified in Section 6.1.5.3 and Section 7.1.3.1.
extensions	See table below
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	-

Extension	Presence	Critical	Content
basicConstraints	Yes	Yes	cA = True pathLenConstraint is not present
authorityKeyIdentifier	Yes	No	keyIdentifier complies with Section 7.1.2.11.1
subjectKeyIdentifier	Yes	No	subjectKeyIdentifier complies with Section 7.1.2.11.4.
keyUsage	Yes	Yes	keyCertSign, crlSign

7.1.2.2. Cross-Certified Subordinate CA Certificate Profile

Currently, Apple Public CA does not issue Cross-Certified Subordinate CA Certificates.

7.1.2.3. Technically Constrained Non-TLS Subordinate CA Certificate Profile

Currently, Apple Public CA does not issue Technically Constrained Non-TLS Subordinate CA Certificates.

7.1.2.4. Technically Constrained Precertificate Signing CA Certificate Profile

Apple Public CA's CA system does not use a Precertificates Signing CA; instead, the Sub-CA that signs the Subscriber Certificates also signs its corresponding Precertificate.

7.1.2.5. Technically Constrained TLS Subordinate CA Certificate Profile

Currently, Apple Public CA does not issue Technically Constrained TLS Subordinate CA Certificates.

7.1.2.6. Unconstrained Subordinate CA Certificate Profiles

Currently, Apple Public CA issues unconstrained Subordinate CA Certificates as they are for itself or its affiliates.

Unconstrained TLS Sub-CA Certificate

Field	Description
tbsCertificate	-
version	v3(2)
serialNumber	A non-sequential number of 128 bits containing at least 64 bits of output from a CSPRNG.
signature	A signature algorithm specified in Section 7.1.3.2.
issuer	Byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1.
validity	notBefore: the value of the certificate signing operation notAfter: a value not to exceed what is specified in Section 6.3.2.

Field	Description
subject	Encoding, length and order is specified in Section 7.1.4.2 Common Name structure is specified in Section 7.1.2.10.2. - Country, - Organization, and - Common Name.
subjectPublicKeyInfo	A key type, size and encoding specified in Section 6.1.5.3 and Section 7.1.3.1.
extensions	See table below
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	-

Unconstrained TLS Sub-CA Extensions

Extension	Presence	Critical	Content
basicConstraints	Yes	Yes	cA = False pathLenConstraint = 0
authorityKeyIdentifier	Yes	No	keyIdentifier complies with Section 7.1.2.11.1
authorityInfoAccess	Yes	No	Access Method OCSP: HTTP URI to the Issuing CA's OCSP responder service
certificatePolicies	Yes	No	- Policy OID 1: 2.23.140.1.2.2 - Policy OID 2: 1.2.840.113635.100.5.19.2.2.2
extKeyUsage	Yes	No	serverAuth
crlDistributionPoints	Yes	No	HTTP URI to CRL complies with Section 7.1.2.11.2
subjectKeyIdentifier	Yes	No	subjectKeyIdentifier complies with Section 7.1.2.11.4
keyUsage	Yes	Yes	keyCertSign, crlSign

Unconstrained S/MIME Sub-CA Certificate

Field	Description
tbsCertificate	-
version	v3(2)
serialNumber	A non-sequential number of 128 bits containing at least 64 bits of output from a CSPRNG.
signature	A signature algorithm specified in Section 7.1.3.2.
issuer	Byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1.

Field	Description
validity	notBefore: the value of the certificate signing operation notAfter: a value not to exceed what is specified in Section 6.3.2.
subject	Encoding, length and order is specified in Section 7.1.4.2 Common Name structure is specified in Section 7.1.2.10.2. - Country, - Organization, and - Common Name.
subjectPublicKeyInfo	A key type, size and encoding specified in Section 6.1.5.3 and Section 7.1.3.1.
extensions	See table below
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	-

Unconstrained S/MIME Sub-CA Extensions

Extension	Presence	Critical	Content
basicConstraints	Yes	Yes	cA = False pathLenConstraint = 0
authorityKeyIdentifier	Yes	No	keyIdentifier complies with Section 7.1.2.11.1
authorityInfoAccess	Yes	No	Access Method OCSP: HTTP URI to the Issuing CA's OCSP responder service
certificatePolicies	Yes	No	Mailbox-validated Strict - Policy OID: 2.23.140.1.5.1.3 Organization-validated Strict - Policy OID: 2.23.140.1.5.2.3 For sub-CA Certificates issued before September 1, 2023 (Note 1): - Policy OID: 1.2.840.113635.100.5.11.5.n - Where n is number between 1-15 inclusive
extKeyUsage	Yes	No	Secure Email, Client Authentication
crlDistributionPoints	Yes	No	HTTP URI to CRL complies with Section 7.1.2.11.2
subjectKeyIdentifier	Yes	No	subjectKeyIdentifier complies with Section 7.1.2.11.4
keyUsage	Yes	Yes	keyCertSign, crlSign

Note 1: The Apple Public CA has issued unconstrained S/MIME Sub-CAs that meet the definition of Extant S/MIME CAs. Those Extant S/MIME CAs may be used to issue compliant S/MIME Certificates until they are replaced by Sub-CAs that comply with the specifications in S/MIME Baseline Requirements by September 15, 2024.

7.1.2.7. Subscriber Certificate Profile

The Apple Public CA issues TLS Server Certificates of type Organization Validated and S/MIME Certificates of types Mailbox-validated Strict and Organization-validated Strict. The following tables summarize the profiles for these Certificate types.

TLS Server Certificates

Field	Description
tbsCertificate	-
version	v3(2)
serialNumber	A non-sequential number of 128 bits containing at least 64 bits of output from a CSPRNG.
signature	A signature algorithm specified in Section 7.1.3.2.
issuer	Byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	notBefore, a value within 24 hours from certificate signing operation notAfter: a value not to exceed what is specified in Section 6.3.2.
subject	Encoding, length and order is specified in Section 7.1.4.2 - Country, - State, - Organization, and - Common Name.
subjectPublicKeyInfo	A key type, size and encoding specified in Section 6.1.5.3 and Section 7.1.3.1.
extensions	See table below
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	-

TLS Server Certificate Extensions

Extension	Presence	Critical	Content
basicConstraints	Yes	Yes	cA = False pathLenConstraint is not present
authorityKeyIdentifier	Yes	No	keyIdentifier complies with Section 7.1.2.11.1

Extension	Presence	Critical	Content
authorityInfoAccess	Yes	No	Access Method OCSP: HTTP URI to the Issuing CA's OCSP responder service Access Method CA Issuers: HTTP URI to the Issuing CA's Certificate
subjectAltName	Yes	No	dnsName (minimum of 1, maximum of 100) (Note 1)
certificatePolicies (Note 2)	Yes	No	- Policy OID 1: 2.23.140.1.2.2 - Policy OID 2: 1.2.840.113635.100.5.19.2.2.2 - CPS Policy Qualifier: "https://www.apple.com/certificateauthority/public" Policy qualifiers also meet the practices specified in Section 7.1.8.
extKeyUsage	Yes	No	serverAuth
crlDistributionPoints	Yes	No	HTTP URI to CRL complies with Section 7.1.2.11.2
subjectKeyIdentifier	Yes	No	subjectKeyIdentifier complies with Section 7.1.2.11.4
keyUsage	Yes	Yes	For RSA keys: Digital Signature, Key Encipherment For ECC Keys: Digital Signature
Signed Certificate Timestamp List	Yes	No	At least three (3) Signed Certificate Timestamps. Complies with Section 7.1.2.11.3
Private Subscriber Extension	Optional	No	One or more extensions that comply with Section 7.1.2.11.5

Note 1: The entry contains either a Fully-Qualified Domain Name or Wildcard Domain Name that the CA has validated in accordance with Section 3.2.2.4. Wildcard Domain Names are validated for consistency with Section 3.2.2.6. The entry does not contain an Internal Name. The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry is composed entirely of P-Labels or Non-Reserved LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System is never included.

Note 2: Certificates issued prior to compliance with Baseline Requirements v2.0 include the userNotice policy qualifier with this content: "Reliance on this certificate by any party assumes acceptance of the Relying Party Agreement found at https://www.apple.com/certificateauthority/public"

S/MIME Certificates

Field	Description
tbsCertificate	-
version	v3(2)
serialNumber	A non-sequential number of 128 bits containing at least 64 bits of output from a CSPRNG.
signature	A signature algorithm specified in Section 7.1.3.2.
issuer	Byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	notBefore, a value within 24 hours from certificate signing operation notAfter: a value not to exceed what is specified in Section 6.3.2.
subject	Subject content varies depending on certificate type (Mailbox-validated Strict, Organization-validated Strict or Pre-S/MIME Baseline Requirements Legacy). Encoding, length and order is specified in Section 7.1.4.2 Mailbox-validated Strict - Email, or - Common Name. Organization-validated Strict - Country, - State, - Organization, - Organization Identifier, - Common Name or Email.
subjectPublicKeyInfo	A key type, size and encoding is specified in Section 6.1.5.3 and Section 7.1.3.1.
extensions	See table below
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	-

S/MIME Certificate Extensions

Extension	Presence	Critical	Content
basicConstraints	Yes	Yes	cA = False pathLenConstraint is not present
authorityKeyIdentifier	Yes	No	keyIdentifier complies with Section 7.1.2.11.1
authorityInfoAccess	Yes	No	Access Method OCSP: HTTP URI to the Issuing CA's OCSP responder service Access Method CA Issuers: HTTP URI to the Issuing CA's Certificate

Extension	Presence	Critical	Content
subjectAltName	Yes	No	rfc822Name (minimum of 1, maximum of 1) (Note 1)
certificatePolicies (Note 2)	Yes	No	Mailbox-validated Strict - Policy OID: 2.23.140.1.5.1.3 Organization-validated Strict - Policy OID: 2.23.140.1.5.2.3 pre-S/MIME Baseline Requirement Certificates – Policy OID: 1.2.840.113635.100.5.11.5.n – Where n is number between 1-15 inclusive All types also include these qualifiers: – CPS Policy Qualifier: "https://www.apple.com/certificateauthority/public" – userNotice Policy Qualifier: "Reliance on this certificate by any party assumes acceptance of the Relying Party Agreement found at https://www.apple.com/certificateauthority/public" Policy qualifiers also meet the practices specified in Section 7.1.8.
extKeyUsage	Yes	No	Mailbox-validated Strict, Organization-validated Strict and pre-S/MIME Baseline Requirement implementation: emailProtection
crlDistributionPoints	Yes	No	HTTP URI to CRL complies with Section 7.1.2.11.2
subjectKeyIdentifier	Yes	No	subjectKeyIdentifier complies with Section 7.1.2.11.4
keyUsage	Yes	Yes	For all types including those pre-S/MIME Baseline Requirement implementation: For RSA keys: – Signing: digitalSignature – Encryption: keyEncipherment – Dual Use: digitalSignature and keyEncipherment For ECC keys: – Signing: digitalSignature – Encryption: keyAgreement – Dual Use: digitalSignature and keyAgreement

Note 1: All Mailbox Addresses in the subject field are repeated as rfc822Name values in the Subject Alternative Name extension.

Note 2: Certificates issued prior to compliance with S/MIME Baseline Requirements v1.0.1 include other Apple-specific reserved policy identifiers outlined in Section 7.1.6.1.

7.1.2.8. OCSP Responder Certificate Profile

This profile covers the OCSP Responder for both Root and Subordinate CAs. Differences are noted in the specific field.

Field	Description
tbsCertificate	-
version	v3(2)
serialNumber	A non-sequential number of 128 bits containing at least 64 bits of output from a CSPRNG.
signature	A signature algorithm specified in Section 7.1.3.2. Selected algorithm mirrors the algorithm used in Certificates for which responses are provided.
issuer	Byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	notAfter: notBefore is the time of signing. notAfter: a value not to exceed what is specified in Section 6.3.2. Certificates issued to responders for a Sub-CA and Root CA have different maximum values.
subject	Fields ordered and encoded as specified in Section 7.1.4.2 - OCSP Responder - Country - Organization, - Common Name.
subjectPublicKeyInfo	A key type, size and encoding is specified in Section 6.1.5.3 and Section 7.1.3.1.
extensions	See table below
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	-

OCSP Responder Certificate Extensions

Extension	Presence	Critical	Content
basicConstraints	No	Yes	cA = False pathLenConstraint is not present
authorityKeyIdentifier	Yes	No	keyIdentifier complies with Section 7.1.2.11.1
authorityInfoAccess	No	-	-

Extension	Presence	Critical	Content
subjectAltName	No	-	-
certificatePolicies	No	-	-
extKeyUsage	Yes	No	id-kp-OCSPSigning
crlDistributionPoints	No	-	-
subjectKeyIdentifier	Yes	No	subjectKeyIdentifier complies with Section 7.1.2.11.4
keyUsage	Yes	Yes	digitalSignature
Signed Certificate Timestamp List	No	-	-
id-pkix-ocsp-nocheck	Yes	No	extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6960, Section 4.2.2.2.1.
Private Subscriber Extension	No	-	-

7.1.2.9. Precertificate Profile

Apple Public CA creates a Precertificate prior to the actual signing of the Certificate, which is used to submit to Certificate Transparency Log operators. The Apple Public CA systems use the Issuing CA to sign both Precertificates and corresponding Certificates.

Field	Description
tbsCertificate	-
version	Encoded value MUST be byte-for-byte identical to the version field of the Certificate
serialNumber	Encoded value MUST be byte-for-byte identical to the serialNumber field of the Certificate
signature	Encoded value MUST be byte-for-byte identical to the signature field of the Certificate
issuer	Encoded value MUST be byte-for-byte identical to the issuer field of the Certificate
validity	Encoded value MUST be byte-for-byte identical to the validity field of the Certificate
subject	Encoded value MUST be byte-for-byte identical to the subject field of the Certificate
subjectPublicKeyInfo	Encoded value MUST be byte-for-byte identical to the subjectPublicKeyInfo field of the Certificate
issuerUniqueID	Encoded value MUST be byte-for-byte identical to the issuerUniqueID field of the Certificate

Field	Description
subjectUniqueID	Encoded value MUST be byte-for-byte identical to the subjectUniqueID field of the Certificate
extensions	See table below.
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the signatureAlgorithm field of the Certificate
signature	-

Precertificate Extensions

Extension	Presence	Critical	Content
Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)	Yes	Yes	An extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.
Signed Certificate Timestamp List	No	-	-
Any other extension	*	*	The order, criticality, and encoded values of all other extensions MUST be byte-for-byte identical to the extensions field of the Certificate

7.1.2.10. Common CA Fields

This section contains several fields that are common among multiple CA Certificate profiles.

7.1.2.10.1. CA Certificate Validity

The Apple Public CA issues Root and Subordinate Certificates with validity that meets the parameters specified in Section 6.3.2.

7.1.2.10.2. CA Certificate Naming

All subject names are encoded as specified in Section 7.1.4.

The Apple Public CA issues Root and Sub-CA Certificates that meet the specification in the table below.

Attribute	Presence	Value
countryName	Yes	US
organizationName	Yes	Apple Inc.

Attribute	Presence	Value
commonName	Yes	For Root Certificates Apple Public [type] [algorithm] Root CA [number] For Sub-CA Certificates Apple Public [type] [algorithm] CA [number] – G[generation] Type: A string identifying the type of Certificates issued under the CA Certificate. For example: "TLS" or "Email". Algorithm: A string representing the algorithm used to generate the Root Certificate Key Pair. For example, "ECC" or "RSA". Number: A numeric value that uniquely distinguishes the CA Certificate from others within the same type/algorithm pair. For Sub-CA Certificates, the number is unique across the entire Root Certificate naming space. Generation: A numeric value that starts with one (1) and increases by one (1) when a new Certificate, that supersedes an existing one, is issued by the same Root Certificate.

7.1.2.11. Common Certificate Fields

This section contains several fields that are common among multiple Subscriber certificate profiles. However, these fields may not be common among all certificate profiles. Subscriber profiles will indicate any differences.

7.1.2.11.1. Authority Key Identifier

Field	Description
keyIdentifier	Always present. It is identical to the subjectKeyIdentifier field of the Issuing CA.
authorityCertIssuer	Never present
authorityCertSerialNumber	Never present

7.1.2.11.2. CRL Distribution Points

The CRL Distribution Points extension is present in Subordinate CA Certificates and Subscriber Certificates. This extension is not present in Root CA Certificates or OCSP Responder Certificates.

When present, the CRL Distribution Points extension contains at least one DistributionPoint and they are formatted as follows:

Field	Presence	Description
distributionPoint	Yes	DistributionPointName is a fullName containing at least one GeneralName of type uniformResourceIdentifier and scheme "http". It contains the HTTP URL of the Issuing CA's CRL for the certificate.
reasons	No	-

Field	Presence	Description
cRLIssuer	No	-

7.1.2.11.3. Signed Certificate Timestamp List

When present, the Signed Certificate Timestamp List extension content is an OCTET STRING containing the encoded SignedCertificateTimestampList, as specified in RFC 6962, Section 3.3.

Each SignedCertificateTimestamp included within the SignedCertificateTimestampList is for a PreCert LogEntryType that corresponds to the current certificate.

7.1.2.11.4. Subject Key Identifier

When present, the subjectKeyIdentifier is the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey, which is compllant with RFC 5280, Section 4.2.1.2.

7.1.2.11.5. Other Extensions

All extensions and extension values not directly addressed by the applicable certificate profile

1. Apply in the context of the public Internet, unless:
    1. The extension OID falls within an OID arc for which the Applicant demonstrates ownership, or,
    2. The Applicant can otherwise demonstrate the right to assert the data in a public context.
2. Do not include semantics that will mislead the Relying Party about certificate information verified by the CA
3. Are DER encoded according to the relevant ASN.1 module defining the extension and extension values.

The following private extensions are used for issuance of a category of TLS Server Certificates. This inclusion is based on an assessment of the reasons provided by the Applicant to establish that the extension can be included.

Extension	Description
Apple Private Extension	Apple Certificate Extensions arc {iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificateExtensions(6)} (1.2.840.113635.100.6)

7.1.3. Algorithm Object Identifiers

7.1.3.1. SubjectPublicKeyInfo

The Apple Public CA and Subscribers use these algorithms to generate Key Pairs:

Algorithm (Object Identifier)	Parameters	Hexadecimal Parameter Encoding
rsaEncryption (1.2.840.113549.1.1.1)	Always present. Content is NULL (explicit)	300d06092a864886f70d0101010500
id-ecPublicKey (1.2.840.10045.2.1)	Always present. Content is namedCurve P-256 key: secp256r1 1.2.840.10045.3.1.7 P-384 key: secp384r1 1.3.132.0.34	 secp256r1: 301306072a8648ce3d020106082a8648ce3d030107 secp384r1: 301006072a8648ce3d020106052b81040022

7.1.3.2. Signature AlgorithmIdentifier

The Apple Public CA may use these signature algorithms and ensures the appropriate signature algorithm and encoding based upon the signing key used.

Algorithm (Object Identifier)	Parameter	Hexadecimal Parameter Encoding
sha256WithRSAEncryption 1.2.840.113549.1.1.11	RSASSA-PKCS1-v1_5 with SHA-256	300d06092a864886f70d01010b0500
sha384WithRSAEncryption 1.2.840.113549.1.1.12	RSASSA-PKCS1-v1_5 with SHA-384	300d06092a864886f70d01010c0500
For P-256 signing key only: ecdsa-with-SHA256 1.2.840.10045.4.3.2	ECDSA with SHA-256	300a06082a8648ce3d040302
For P-384 signing key only: ecdsa-with-SHA384 1.2.840.10045.4.3.3	ECDSA with SHA-384	300a06082a8648ce3d040303

7.1.4. Name Forms

This section details encoding rules that apply to all Certificates issued by Apple Public CA.

7.1.4.1. Name Encoding

For all Certificates issued under this CPS, the encoded content of the Issuer DN matches byte-for-byte the encoded form of the Subject DN field of its Issuing CA Certificate.

For each CA Certificate in the Certification Path, the encoded content of the Subject DN field of a Certificate matches byte-for-byte identical all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

Apple Public CA encodes Certificates ensuring that:

- Each Name contains an RDNSequence.
- Each RelativeDistinguishedName contains exactly one AttributeTypeAndValue.
- Each RelativeDistinguishedName, when present, is encoded within the RDNSequence in the order that it appears in Section 7.1.4.2.
- Each Name MUST NOT contain more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames unless explicitly allowed in Baseline Requirements and documented in this CPS.

7.1.4.2. Subject Attribute Encoding

Apple Public CA includes the Subject attributes in the tables below in Root CA, Subordinate CA, Subscriber and OCSP Responder Certificates. These attributes are included in a Certificate only after validation is completed in accordance with Section 3.2.

Currently, Apple Public CA does not include IP addresses in its Certificates. Domain Names are included as specified in Section 3.2.2. Subject DN fields only with metadata such as ".", "-", and " " (i.e., space) characters are not allowed.

Root CA and Sub-CA Certificates

Attribute	Encoding (Note 1)	Max Length	Presence
countryName	PrintableString	2	Yes
organizationName	UTF8String or PrintableString	64	Yes
commonName	UTF8String or PrintableString	64	Yes

Note 1: For Root CA and Sub-CA Certificates issued prior to implementing Baseline Requirements version 2.0, the preferred encoding was PrintableString.

TLS Server Certificates

The table below describes the attribute order, maximum length and encoding type used by TLS Server Certificates issued starting no later than September 15, 2023.

Attribute (Note 1)	Encoding (Note 2)	Max Length	Presence
countryName	PrintableString	2	Yes
stateOrProvinceName	UTF8String or PrintableString	128	Yes
organizationName	UTF8String or PrintableString	64	Yes
commonName	UTF8String or PrintableString	64	Yes

Note 1: For TLS Server Certificates issued prior to implementing Baseline Requirements version 2.0, the attribute order may differ.

Note 2: For TLS Server Certificates issued prior to implementing Baseline Requirements version 2.0, the preferred encoding was PrintableString.

S/MIME Certificates

The table below applies to S/MIME Certificates issued after September 1, 2023. Certificates issued prior to this date did not include the emailAddress and organizationIdentifier fields.

Attribute	Encoding	Max Length	Presence (Note 1)	
			MVS	OVS
countryName	PrintableString	2	-	Yes
stateOrProvinceName	UTF8String or PrintableString	128	-	Yes
organizationName	UTF8String or PrintableString	64	-	Yes
organizationIdentifier (Note 2)	UTF8String or PrintableString	None	-	Yes
emailAddress (Note 3)	IA5String	255	Yes	No
commonName (Note 3)	UTF8String or PrintableString	64	No	Yes

Note 1: Mailbox-validated Strict (MVS), Organization-validated Strict (OVS).

Note 2: The organization Identifier is populated with the result of the verification performed in accordance with Section 3.2.2. The value is constructed using the instructions outlined in Appendix C - Registration Schemes for Organization Identifier in S/MIME Certificates, and identifies both the scheme/method used and the resulting identifier.

Note 3: Certificates will include either the emailAddress or commonName field but not both. The specific attribute is selected depending on Mailbox Address to allow issuance for addresses longer than 64 characters and whether a specific implementation requires it.

OCSP Responder Certificates

Attribute	Encoding	Max Length	Presence
countryName	PrintableString	2	Yes
organizationName	UTF8String or PrintableString	64	Yes
commonName	UTF8String or PrintableString	64	Yes

7.1.4.3. Subscriber and OCSP Responder Certificate Common Name Attribute

TLS Server Certificates

The commonName attribute is present and mirrors one value contained in the subjectAltName extension. Since Apple Public CA does not issue Certificates with IP addresses, the commonName value is either a Fully-Qualified Domain Name or a Wildcard Domain Name.

The value is encoded as a character-for-character copy of the dNSName entry value from the Subject Alternative Name extension. All Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name are encoded as LDH Labels, and P-Labels are not converted to their Unicode representation.

S/MIME Certificates

The Mailbox Address contained in the Subject DN commonName field, or emailAddress, is mirrored as a GeneralName entry of type rfc822Name in the subjectAltName extension.

The Apple Public CA does not issue Certificates with a Personal Name therefore the commonName field is not populated with information other than the Mailbox Address.

OCSP Responder Certificates

The commonName attribute is present and reflects a combination of the Sub-CA's commonName, a unique identifier including a date component and the string “OCSP Responder”.

7.1.4.4. Subscriber Certificate Subject Alternative Name

Certificates contain the Subject Alternative Name Extension.

For TLS Server Certificates this extension is populated with at least one dnsName entry. Prior to issuing the Certificate, each dNSName is confirmed to be either a Wildcard Domain Name or FQDN. Every Domain Label in the dNSName is

confirmed to be an LDH Label that conforms to the specification for a P-Label or a Non-Reserved LDH Label.

The Apple Public CA does not currently include iPAddress entries.

For S/MIME Certificates this extension is populated with the rfc822Name.

Field	Certificate Type		Value (Example)
	OV	S/MIME	
dNSName	Required		A verified Wildcard Domain Name or FQDN Internal Names are not allowed The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry MUST be composed entirely of P-Labels or Non-Reserved LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System MUST NOT be included
rfc822Name	—	Required	Verified Mailbox Address

7.1.4.5. Other Subject Attributes

Apple Public CA does not include attributes other than those documented in Section 7.1.4.2.

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

Certificates issued by the Apple Public CA that contain the CertificatePolicy extension in accordance with Section 7.1.2 are populated with at least one policy OID.

Policy OIDs included in Certificates are specified in the table below and mirror the Apple Public Root CP Section 7.1.6.1.

7.1.6.1. Reserved Certificate Policy Identifiers

The following policy OIDs are reserved by the CAB Forum and the Apple Public CA as a means of asserting that a Certificate complies with the Baseline

Requirements and S/MIME Baseline Requirements as outlined in the Apple Public Root Cp. Only those policy OIDs that have been or are currently used are listed.

7.1.6.1.1. CAB Forum Reserved

TLS Server Certificates

Organization Validated

{joint-iso-itu-t(2) international-organizations(23) ca-browser- forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)

S/MIME Certificates

Mailbox-validated: Subject is limited to (optional) subject:emailAddress and/or subject:serialNumber attributes

Organization-validated: Includes only Organizational (Legal Entity) attributes in the Subject.

In addition, Generations (known as Legacy, Multipurpose, and Strict) are specified for each of these Certificate Types, acknowledging both the current diversity of practice in issuing S/MIME Certificates as well as the desire to move towards more closely-defined practices over time.

Mailbox-validated

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) legacy (1)} (2.23.140.1.5.1.1),

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) multipurpose (2)} (2.23.140.1.5.1.2), and

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) strict (3)} (2.23.140.1.5.1.3).

Organization-validated

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) legacy (1)} (2.23.140.1.5.2.1),

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) multipurpose (2)} (2.23.140.1.5.2.2), and

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) strict (3)} (2.23.140.1.5.2.3).

7.1.6.1.2. Apple Reserved

TLS Server Certificates

For TLS Server Certificates, when a CAB Forum reserved policy OID is included, its equivalent Apple reserved policy OID is also included.

Organization Validated

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) applePublicRootCertificatePolicyID (19) apple-public-device (2) baseline-requirements(2) organization-validated(2)} (1.2.840.113635.100.5.19.2.2.2)

S/MIME Certificates

Pre-S/MIME Baseline Requirements Sponsor Validated

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleISTEmailCertificatePolicyIDs (5) signEncrypt (1)} (1.2.840.113635.100.5.11.5.1),

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleISTEmailCertificatePolicyIDs (5) Sign (2)} (1.2.840.113635.100.5.11.5.2),

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleISTEmailCertificatePolicyIDs (5) Encrypt (3)} (1.2.840.113635.100.5.11.5.3), and

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleISTEmailCertificatePolicyIDs (5) (n)} (1.2.840.113635.100.5.11.5.*5-15*); where n may be a number between 4 and 15 inclusive.

7.1.6.1.3. Reserved Policy OIDs Equivalence

The table below shows policy OIDs that equivalent. Apple Public CA will include the CAB Forum reserved policy OIDs and may include the equivalent reserved Apple policy OID in Certificates.

Certificate Type	CAB Forum Reserved	Apple or Vendor Reserved
TLS - Organization Validated	2.23.140.1.2.2	1.2.840.113635.100.5.19.2.2.2
S/MIME - Mailbox Validated Strict	2.23.140.1.5.1.3	-

Certificate Type	CAB Forum Reserved	Apple or Vendor Reserved
S/MIME - Organization Validated Multipurpose	2.23.140.1.5.2.2	-
S/MIME - Organization Validated Strict	2.23.140.1.5.2.3	-
S/MIME Only Sign and Encrypt	-	1.2.840.113635.100.5.11.5.1
S/MIME Only Sign	-	1.2.840.113635.100.5.11.5.2
S/MIME Only Encrypt	-	1.2.840.113635.100.5.11.5.3
Future Use	-	1.2.840.113635.100.5.11.5.*n* where *n* may be a number between 4 and 15, inclusive

7.1.6.2. Root CA Certificates

The Apple Public CA does not include the certificatePolicies extension in its Root Certificates.

7.1.6.3. Subordinate CA Certificates

The Apple Public CA issues Sub-CA Certificates with either:

1. One or more explicit policy identifiers defined in Section 7.1.6.1, or
2. The anyPolicyidentifier(2.5.29.32.0).

7.1.6.4. Subscriber Certificates

The Apple Public CA includes some policy OIDs in its Subscriber Certificates. Those policy OIDs are documented in Section 7.1.6.1

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

The Apple Public CA includes the qualifier of type id-qt-cps (OID: 1.3.6.1.5.5.7.2.1) containing a HTTPS URL for the Repository with this CPS in all Subscriber Certificates.

TLS Server Certificates issued before September 15, 2023 and S/MIME Certificates may include a qualifier of type id-qt-unotice (OID: 1.3.6.1.5.5.7.2.2) with a statement explaining conditions for reliance by a Relying Party in the explicitText field.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

Apple Public CA issues CRLs from its Roots and Sub-CAs that meet the specification below.

Field	Description
tbsCertList	-
version	v2(1)
signature	A signature algorithm specified in Section 7.1.3.2.
issuer	Byte-for-byte identical to the subject field of the Issuing CA.
thisUpdate	Indicates the issue date of the CRL in UTCTime.
nextUpdate	Indicates the date in UTCTime by which the next CRL will be issued. Specific parameters for Root and sub-CA issuance are in Section 4.9.7.
revokedCertificates	See detail in revokedCertificates Component table below. This field is present when a Certificate has been revoked and its associated entry is included. An entry is removed after it has appeared on at least one regularly scheduled CRL beyond the revoked Certificate's validity period.
crlExtensions	See Section 7.2.2.
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertList.signature.
signature	-

"revokedCertificates" Component Specification

Component	Presence	Description
CertificateSerialNumber	Yes	Byte-for-byte identical to the CertificateSerialNumber contained in the revoked Certificate (or in cases that a Precertificate was generated but no Certificate was created, the Precertificate's serial number)

Component	Presence	Description
revocationDate	Yes	Date and time, in UTCTime, when revocation occurred. Exceptionally when subsequently determined that the key was compromised prior to the initial revocation date, an updated date reflecting when the key was considered compromised.
crlEntryExtensions: reasonCode	Conditional	Indicates the most appropriate reason for revocation of the Certificate, it is not marked critical when present: For Sub-CA issued CRLs (See Note 1) • superseded • cessationOfOperation • affiliationChanged (See Note 2) • keyCompromise • privilegeWithdrawn (See Note 2) For Root CA issued CRLs • superseded • cessationOfOperation • affiliationChanged These reason codes are not included: • certificateHold • unspecified (See Note 3)

Note 1: Reason Codes are selected by the Subscriber or the Apple Public CA based on guidance provided in Appendix D.

Note 2: The privilegeWithdrawn and affiliationChanged reason codes are not made available for selection by the Subscriber as only the Apple Public CA can conclusively determine reasons resulting in these reason codes.

Note 3: Selecting the unspecified reason code option results in the reasonCode CRL entry extension being omitted from the CRL entry.

7.2.1. Version Number

CRLs issued by the Apple Public CA conform to the X.509 version 2 format.

7.2.2. CRL and CRL Entry Extensions

CRLs will include the "Required" extensions but may omit "Conditional" ones.

CRL Entry Extension	Critical	Required/ Conditional	Value
Authority Key Identifier	No	Required	keyIdentifier contains Identifier to Issuing CA's Private Key. It complies with Section 7.1.2.11.1

CRL Entry Extension	Critical	Required/ Conditional	Value
CRL Number	No	Required	Prior to March 15, 2024 Monotonically increasing sequence number After March 15, 2024 An INTEGER greater than or equal to zero (0) and less than 2^{159}, and conveys a strictly increasing sequence.
Issuing Distribution Point (Note 1)	Yes	Conditional (Note 2)	The distributionPoint field contains a HTTP URL to CRL

Note 1: Issuing Distribution Point is used only for Sub-CA issued CRLs.

Note 2: Issuing Distribution Point is Required when a CRL does not contain all the entries for revoked unexpired certificates issued by the CRL issuer.

7.3. OCSP PROFILE

7.3.1. Version Number

OCSP responses conform to version 1 in RFC 6960.

OCSP responses provided by an OCSP Responder from a Root CA will include the following fields:

Field	Value
Signature Algorithm	A signature algorithm specified in Section 7.1.3.2.
thisUpdate	Time at which the status indicated is known to the responder to be correct
nextUpdate	Time at which newer information will be available
Responder's Identifier	OCSP Responder's Public Key SHA1 hash
Produced At	Time when the response was signed
Response for each Certificate	Certificate Identifier: hashes of the issuer's DN and Public Key, and the Certificate's serial number Certificate Status: Good: for valid Certificates. Revoked: for revoked Certificates. The revocationReason field within the RevokedInfo of the CertStatus is present and is populated with the same values for a CRL issued by a Root CA described in Section 7.2.2. Unknown: for Certificates not known to the Root CA.

OCSP responses provided by an OCSP Responder from a Subordinate CA will include the following fields:

Field	Value
Signature Algorithm	A signature algorithm specified in Section 7.1.3.2.
thisUpdate	Time at which the status indicated is known to the responder to be correct
nextUpdate	Time at which newer information will be available
Responder's Identifier	OCSP Responder's Public Key SHA1 hash
Produced At	Time when the response was signed
Response for each Certificate	Certificate Identifier: hashes of the issuer's DN and Public Key, and the Certificate's serial number Certificate Status: Good: for valid Certificates and Precertificates (with no assigned Certificate) Revoked: for revoked Certificates (or a Precertificate for which a Certificate was not created). When reason codes are used, the revocationReason field within the RevokedInfo of the CertStatus is present and is populated with the same values in Section 7.2.2. Unknown: for Certificates not known to the issuing CA

7.3.2. OCSP Extensions

OCSP responses issued by Sub-CAs or delegated responders will meet the following:

OCSP Extension	Critical	Required/Optional
Nonce	No	Required (if present in request)

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

An audit is performed by an independent external auditor to assess the adequacy of the Apple Public CA's business practices disclosure and compliance with this CPS for all CAs technically capable of issuing publicly trusted Certificates. The audit is performed annually and executed in a way that prevents unaudited periods from one audit to the next starting from the CA Key Pair generation until the expiration or revocation of all Certificates associated to it.

For Root, Sub-CA, and TLS Server Certificates, the auditor will also assess controls to the then-current standards:

- CPA Canada Trust Service Principles and Criteria for Certification Authorities, and
- CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security.

For S/MIME Certificates, the auditor will also assess controls to the current standard:

- CPA Canada WebTrust Service Principles and Criteria for Certification Authorities S/MIME Certificates.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The auditors performing the annual audit are from an independent audit firm that is approved to audit according to CPA Canada WebTrust for Certification Authorities Principles and Criteria.

The Apple Public CA ensures its WebTrust auditors meet the requirements of Section 8.2 of the Apple Public Root CP and Mozilla Root Store Policy Section 3.2.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The Apple Public CA will retain an independent external audit firm.

8.4. TOPICS COVERED BY ASSESSMENT

The audit will meet the requirements of the audit schemes identified in Section 8.1.

The Apple Public CA's compliance team ensures that the audit is conducted in accordance with the latest version of the schemes defined in Section 8.1.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

8.6. COMMUNICATION OF RESULTS

The Apple Public CA works with its auditor to ensure audit reports conform with the content and format requirements in the Apple Public Root CP Section 8.6. Audit results are communicated to the Apple CA Policy Authority and to others as deemed appropriate based on agreements, regulations, and law. The Apple Public CA submits audit results to its Application Software Suppliers.

Copies of the latest audit reports can be found in the Apple Public CA's Repository as specified in Section 2.1. The Apple Public CA publishes them no later than 3 months from the end of the audit period; otherwise, it works with the Root CA, Application Software Providers and the auditors to provide a satisfactory explanation.

8.7. SELF-AUDITS

On at least a quarterly basis, the Apple Public CA performs regular internal audits against at least three percent (3%) of Certificates issued since the last internal audit.

Root Certificates

The Apple Public CA validates Root Certificates issued for compliance to profiles and naming structures as specified in Section 7, and verifies adherence to key sizes and algorithms as specified in Section 6.

Sub-CA Certificates

The Apple Public CA validates Sub-CA Certificates issued for compliance to profiles and naming structures as specified in Section 7, and verifies adherence to key sizes and algorithms as specified in Section 6.

Subscriber and OCSP Responder Certificates

The Apple Public CA automatically validates all Subscriber and OCSP Responder Certificates issued for compliance to profiles and naming structures as specified in Section 7, and verifies adherence to key sizes and algorithms as specified in Section 6.

8.8. REVIEW OF DELEGATED PARTIES

The Apple Public CA documents the Enterprise RA obligations in the Terms of Use or Subscriber Agreement and other information material (e.g., training manuals or specifications). The enrollment system is configured to verify those obligations for each Certificate Application submitted by the Enterprise RA. At least annually, those controls are evaluated to ensure they still cover all obligations and are still effective.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

The Apple Public CA reserves the right to charge Subscriber fees for Certificate issuances and renewals. The Apple Public CA may change its fees at any time in accordance with the applicable Subscriber agreement.

9.1.2. Certificate Access Fees

The Apple Public CA reserves the right to charge a fee for making a Certificate available or for access to its Certificate databases.

9.1.3. Revocation or Status Information Access Fees

The Apple Public CA does not charge a Certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL. The Apple Public CA reserves the right to charge a fee for providing customized CRLs or other value-added revocation and status information services.

9.1.4. Fees for Other Services

The Apple Public CA does not charge a fee for access to this CPS or for simply viewing the document. Any additional use of this CPS including but not limited to reproduction, redistribution, modification, or creation of derivative works, may be subject to a license agreement with the entity holding the copyright to the document. The Apple Public CA reserves the right to charge for any other additional or future services not currently outlined in this CPS.

9.1.5. Refund Policy

No stipulation.

9.2. FINANCIAL RESPONSIBILITY

To the extent permitted by applicable law Apple disclaims any warranties, including any warranty of merchantability or fitness for a particular purpose. All relying parties must bear the risk of reliance on any Certificates issued by the Apple Public CA.

9.2.1. Insurance Coverage

Apple maintains general liability insurance coverage.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

The following information is considered Apple confidential and protected against disclosure using a reasonable degree of care and may not be disclosed:

- Private Keys and data used to access the CA system,
- Business and security plans including but not limited to business continuity, incident response, contingency, and disaster recovery plans,
- Security mechanisms used to protect the confidentiality, integrity, or availability of information,
- Information held by the Apple Public CA as personal or non-public information in accordance with Section 9.4, and
- Transaction records, audit logs, archival records, financial audit records, and external or internal audit trail records and any audit reports.

9.3.2. Information Not Within the Scope of Confidential Information

The following information shall not be considered confidential:

- Information included in Certificates,
- Root Certificates and Sub-CA Certificates,
- Information contained in this CPS, and
- Any Certificate status or Certificate revocation reason code.

9.3.3. Responsibility To Protect Confidential Information

Confidential information will not be released to any third parties unless required by law or requested by a court with jurisdiction over the Apple Public CA. Apple's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information. The confidential information will be kept confidential even after the termination of this CPS.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

The Apple Public CA follows the Apple privacy policy which is available at https://www.apple.com/legal/privacy.

9.4.2. Information Treated as Private

See Section 9.4.1.

9.4.3. Information Not Deemed Private

Any information publicly available through a Certificate, CRL or their contents is not deemed private.

9.4.4. Responsibility To Protect Private Information

See Section 9.4.1.

9.4.5. Notice and Consent To Use Private Information

See Section 9.4.1.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

See Section 9.4.1.

9.4.7. Other Information Disclosure Circumstances

See Section 9.4.1.

9.5. INTELLECTUAL PROPERTY RIGHTS

Apple and/or its business partners own the intellectual property rights in Apple Public CA's services, including the Certificates, CRLs, trademarks used in providing the services, the policies and procedures supporting the operations of such services, the CA infrastructure, information provided via OCSP, and this CPS. Apple, iOS, and macOS are trademarks of Apple Inc., in the United States and other countries. Apple grants permission to reproduce and distribute Certificates on a nonexclusive and royalty-free basis, provided that they are reproduced and distributed in full. Private Keys and Public Keys remain the property of the Subscribers who rightfully hold them. All secret shares (distributed elements) of the Apple Private Keys are the property of Apple.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, Apple does not make any representations regarding its products or services. To the extent permitted by applicable law Apple disclaims any warranties, including any warranty of merchantability or fitness for a particular purpose.

Subject to the terms and conditions of this CPS and any applicable agreement between the parties, Apple represents to Subscribers that they:

- Comply in all material aspects with this CPS, and all applicable laws and regulations,
- Have verified all Certificates issued by the Apple Public CA using the processes outlined in this CPS,
- Publish and update CRLs and OCSP responses on a regular basis,

- Meet the minimum requirements in the CAB Forum Baseline Requirements, and
- Maintain a Repository of public information on its website (See Section 2.1).

9.6.2. RA Representations and Warranties

Subject to the terms and conditions of this CPS and any applicable agreement between the parties, RAs represent that:

- The RA's Certificate issuance and management services conform to this CPS, and
- All Certificates requested by the RA meet the requirements of this CPS.

9.6.3. Subscriber Representations and Warranties

Subscribers are solely responsible for any information provided as part of a Certificate Application and for all transactions that use the Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify the Apple Public CA if a change occurs that could affect the status of the Certificate, or if they believe that the Certificate information or Private Key have been compromised or are no longer valid or secure.

Apple's Subscriber Terms of Use includes the following Subscriber requirements and obligations:

- Securely generating its Private Keys and protecting its Private Keys from compromise,
- Providing accurate and complete information when communicating with the Apple Public CA,
- Confirming the accuracy of the Certificate data prior to using the Certificate,
- Promptly
  - Informing themselves of the reasons for revoking a Certificate as described in this CPS's Appendix D, and, acknowledging understanding of them,
  - requesting revocation of a Certificate, cease using it and its associated Private Key, and notify the Apple Public CA if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate, and
  - requesting revocation of the Certificate, and ceasing using it, if any information in the Certificate is or becomes incorrect or inaccurate,
- Ensuring that individuals managing Certificates on behalf of an organization have received security training appropriate to the Certificate,

- Using the Certificate only for authorized and legal purposes, consistent with the Certificate purpose, this CPS, and the relevant Subscriber Terms of Use, and
- Promptly cease using the Certificate and related Private Key after the Certificate's expiration.

Subscriber Agreements may include additional representations and warranties.

9.6.4. Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a Certificate issued by the Apple Public CA, it:

- Obtained sufficient knowledge on the use of Certificates and PKI,
- Studied the applicable limitations on the usage of Certificates and agrees to Apple's limitations on liability related to the use of Certificates,
- Has read, understands, and agrees to the Apple Relying Party Agreement and this CPS,
- Verified all Certificates in the certificate chain using the relevant CRL or OCSP,
- Will not use an expired or revoked Certificate, and
- Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a Certificate after considering:
    - applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction,
    - the intended use of the Certificate as listed in the Certificate or this CPS,
    - the data listed in the Certificate,
    - the economic value of the transaction or communication,
    - the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
    - the Relying Party's previous course of dealing with the Subscriber,
    - the Relying Party's understanding of trade, including experience with computer-based methods of trade, any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction, and
    - any unauthorized reliance on a Certificate is at the party's own risk.

Relying Party Agreements may include additional representations and warranties.

9.6.5. Representations and Warranties of Other Participants

The parties agree that there are no third-party beneficiaries, other than those specifically identified herein under this CPS and any other applicable agreement or Terms of Use.

9.7. DISCLAIMERS OF WARRANTIES

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, APPLE DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. APPLE DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. APPLE DOES NOT GUARANTEE THE AVAILABILITY OF ANY PRODUCTS OR SERVICES AND MAY MODIFY OR DISCONTINUE ANY PRODUCT OR SERVICE OFFERING AT ANY TIME.

9.8. LIMITATIONS OF LIABILITY

ANY ENTITY USING AN APPLE CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF APPLE RELATED TO SUCH USE, PROVIDED THAT THE APPLE PUBLIC CA HAS MATERIALLY COMPLIED WITH THIS CPS IN PROVIDING THE CERTIFICATE OR SERVICE. APPLE'S LIABILITY FOR CERTIFICATES AND SERVICES THAT DO NOT MATERIALLY COMPLY WITH THIS CPS IS LIMITED AS SET FORTH IN THE APPLE RELYING PARTY AGREEMENT. THEY FURTHER ACKNOWLEDGE THAT THE CERTIFICATES ARE NOT INTENDED OR SUITABLE FOR USE IN SITUATIONS OR ENVIRONMENTS WHERE THE FAILURE OR TIME DELAYS OF, OR ERRORS OR INACCURACIES IN THE CONTENT, DATA OR INFORMATION PROVIDED BY, THE CERTIFICATES AND SERVICES COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE, INCLUDING WITHOUT LIMITATION THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT OR WEAPONS SYSTEMS.

All liability is limited to actual and legally provable damages. Apple is not liable for:

- Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if Apple is aware of the possibility of such damages,
- Liability related to fraud or willful misconduct of the Applicant,
- Liability related to use of a Certificate that exceeds the limitations on use, value, or transactions as stated either in the Certificate, this CPS or any applicable Subscriber or Relying Party agreement,
- Liability related to the security, usability, or integrity of products not supplied by Apple, including the Subscriber's and Relying Party's software or hardware, or

- Liability related to the compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether Apple failed to follow any provision of this CPS, or (v) whether any provision of this CPS was proven ineffective.

The disclaimers and limitations on liabilities in this CPS are fundamental terms to the use of Certificates and services provided by the Apple Public CA.

To the extent the Apple Public CA has issued and managed the Certificate(s) at issue in compliance with this CPS, Apple shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit Apple's and the applicable Affiliates' liability. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages.

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber Agreements.

The liability (and/or limitation thereof) of Enterprise RAs and the Apple Public CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9. INDEMNITIES

9.9.1. Indemnification by Apple

To the extent permitted by applicable law, Apple shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by an Application Software Vendor related to a Certificate issued by the Apple Public CA, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either (1) a valid and trustworthy Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) a Certificate that has expired or (ii) a revoked Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status. Such Indemnification responsibilities shall be limited by the monetary limitation of liability amounts identified in the applicable agreements.

9.9.2. Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify Apple, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable

attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence or intentional acts; (iv) Subscriber's misuse of the Certificate or Private Key; or (v) failure to notify the Apple Public CA that the Private Key and its accompanying Certificate have been compromised or are no longer valid.

The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.3. Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify Apple, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Relying Party , regardless of whether the misrepresentation or omission was intentional or unintentional; (ii)Relying Party's breach of the Relying Party Agreement, this CPS, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Relying Party's negligence or intentional acts; (iv)Relying Party's misuse of the Certificate or Private Key, or (v) failure to notify the Apple Public CA that the Private Key and its accompanying Certificate have been compromised or are no longer valid.

The applicable Relying Party Agreement may include additional indemnity obligations.

9.10. TERM AND TERMINATION

9.10.1. Term

The CPS and/or Relying Party Agreement, and any amendments thereto, become effective upon publication to the Repository (See Section 2.1). The CPS and relevant agreements will continue until either an updated version is published to the Repository, (see Section 2.1), or they are terminated in accordance with the CPS or the termination provisions of the applicable agreement.

9.10.2.Termination

This CPS is amended from time to time, and shall remain in effect until replaced by a newer version.

9.10.3.Effect of Termination and Survival

Upon termination of this CPS, Subscriber Agreement and/or Relying Party Agreement, Subscribers and Relying Parties are nevertheless bound by their terms for all Certificates issued for the remainder of the validity periods of such Certificates, until replaced by newer versions of those documents.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The notice provisions for this CPS are outlined in Section 2.2. Notices are deemed effective only after acknowledgment of receipt from Apple. Apple may provide notice and provide updates to this CPS, Subscriber Agreement and/or Relying Party Agreement by making them publicly available in the Repository, see Section 2.1. Notices and updates to this CPS by Apple are deemed effective upon public availability in the Repository.

Notices to Application Software Vendors are sent out in accordance with the respective requirements.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

This CPS is reviewed as frequently as necessary, but at least once a year. This CPS, Subscriber Agreement, and/or Relying Party Agreement may be amended at any time without prior notice. The latest CPS is made publicly available in the Repository (See Section 2.1). Updates supersede any designated or conflicting provisions of the referenced version of the CPS. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the Apple CA Policy Authority.

9.12.2.Notification Mechanism and Period

Apple Public CA posts CPS revisions to its Repository (See Section 2.1). The Apple Public CA may make changes to this CPS without notice.

9.12.3.Circumstances Under Which OID Must Be Changed

The Apple CA Policy Authority is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13. DISPUTE RESOLUTION PROVISIONS

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.

Parties are required to notify the Apple Public CA and attempt to resolve disputes directly with the Apple Public CA before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14. GOVERNING LAW

Under this CPS, the rights and obligations of the parties shall be governed by and construed and enforced under the laws of the State of Delaware, without regard to its choice of law principles, except that the arbitration clause below, and any arbitration

hereunder, shall be governed by the United States Federal Arbitration Act, Chapters 1 and 2. The Convention on Contracts for the International Sale of Goods shall not apply to this CPS.

9.15. COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to all applicable laws and regulations.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

This CPS, the Terms of Use and the applicable agreement represents the entire agreement, and contractually obligates each Subscriber, Relying Party and RA to comply with this CPS and applicable industry guidelines. The Apple Public CA also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. Third parties may not rely on or bring action to enforce such agreement.

9.16.2. Assignment

Entities operating under this CPS may not assign their rights or obligations without the prior written consent of Apple. Any assignment made in violation of this section shall be voided upon Apple's request.

9.16.3. Severability

If a provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

Apple may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. Apple's failure to enforce a provision of this CPS does not waive Apple's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by Apple.

9.16.5. Force Majeure

Apple is not liable for a delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond Apple's reasonable control. The operation of the Internet is beyond Apple's reasonable control.

9.17. OTHER PROVISIONS

No stipulation.

Appendix A: Apple Root and Subordinate CAs Hierarchy

This table lists all valid Root Certificate and Sub-CA Certificates issued by the Apple Public CA. The list is organized alphabetically using the Root Certificate Common Name first and then Sub-CA Certificate Common Name.

Root Certificate Common Name	Sub-CA Certificate Common Name	Certificate Serial Number	Type of Subscriber Certificates Issued
Apple Public Email ECC Root CA 1	N.A. This is a Root CA.	77:3C:5E:3F:B7:F6:9B:83:9A:F9:FA:3D:DA:98:C1:27	Sub-CA Certificates for SMIME
Apple Public Email RSA Root CA 1	N.A. This is a Root CA.	30:1D:C3:12:31:84:00:48:2C:40:18:C3:40:3B:A0:06	Sub-CA Certificates for SMIME
Apple Public TLS ECC Root CA 1	N.A. This is a Root CA.	4F:EE:9B:14:C1:59:DA:15:BB:9E:F0:D6:D1:72:9C:DF	Sub-CA Certificates for TLS
Apple Public TLS RSA Root CA 1	N.A. This is a Root CA.	23:ED:5C:70:CD:8E:EA:F6:36:6C:BF:C5:F6:63:0B:AA	Sub-CA Certificates for TLS
Apple Public Email ECC Root CA 1	Apple Public Email ECC CA 1 - G1	52:D6:53:71:84:53:65:95:FF:7B:70:BF:8A:B6:0F:71	S/MIME Certificates
	Apple Public Email ECC CA 1 - G2	7C:37:00:C4:11:C2:2D:3A:0A:53:5C:FA:37:2F:78:4C	S/MIME Certificates
Apple Public Email RSA Root CA 1	Apple Public Email RSA CA 1 - G1	19:9C:EA:8C:B9:3D:3C:62:9A:27:6A:E7:EC:BB:8E:17	S/MIME Certificates
	Apple Public Email RSA CA 1 - G2	04:9C:D0:F1:65:DE:D6:D5:38:03:AB:F8:72:C2:C3:8B	S/MIME Certificates
Apple Public TLS ECC Root CA 1	Apple Public TLS ECC CA 1 - G1	63:C9:4D:74:A4:AB:93:80:22:8D:30:27:41:5E:06:66	TLS Server Certificates
Apple Public TLS RSA Root CA 1	Apple Public TLS RSA CA 1 - G1	2A:BF:99:F3:ED:8E:06:0C:19:4E:9A:77:F1:12:B9:E2	TLS Server Certificates
Apple Public Email ECC Root CA 2	N.A. This is a Root CA.	42:8D:05:CB:4A:B8:5E:24:50:8C:B5:97:FB:CF:3C:AF	Sub-CA Certificates for SMIME
Apple Public Email RSA Root CA 2	N.A. This is a Root CA.	76:FC:46:52:74:12:6C:E0:DE:13:63:94:03:20:EA:1F	Sub-CA Certificates for SMIME
Apple Public TLS ECC Root CA 2	N.A. This is a Root CA.	2F:9C:B2:A8:73:D4:70:08:BD:43:49:93:0F:E4:7A:44	Sub-CA Certificates for TLS
Apple Public TLS RSA Root CA 2	N.A. This is a Root CA.	0F:64:18:4C:D1:05:31:00:8C:A5:8A:58:DF:FB:4F:39	Sub-CA Certificates for TLS
Apple Public Email ECC Root CA 2	Apple Public Email ECC CA 2 - G1	21:45:5A:75:FA:BC:B2:5D:AC:22:00:4F:2C:42:CE:43	S/MIME Certificates
Apple Public Email RSA Root CA 2	Apple Public Email ECC CA 2 - G1	0C:A0:30:10:10:39:04:19:ED:5E:4C:2F:4C:06:BB:6F	S/MIME Certificates

Root Certificate Common Name	Sub-CA Certificate Common Name	Certificate Serial Number	Type of Subscriber Certificates Issued
Apple Public TLS ECC Root CA 2	Apple Public TLS ECC CA 2 - G1	01:D6:17:F2:AC:2B:85:09:CA:1F:A3:36:F1:ED:3E:49	TLS Server Certificates
Apple Public TLS RSA Root CA 2	Apple Public TLS RSA CA 2 - G1	21:BA:9F:8A:1E:06:D5:5A:D0:E3:D4:59:CD:4B:F0:8E	TLS Server Certificates

Appendix B: Verification Sources

Sources List

Ordered alphabetically by Jurisdiction

Jurisdiction	Agency Information
StateOrProvinceName For: California CountryName: For: United States	**Name:** California Secretary of State **Website:** https://bizfileonline.sos.ca.gov/search/business **Registration Number Format:** (Entity Number) For corporations: The letter C followed by an entity number that is at least a 7-digit number. For example: C1234567 For a limited liability company or limited partnership: A 12-digit entity number. For example: 123456789012
StateOrProvinceName For: Delaware CountryName: For: United States	**Name:** State of Delaware, Department of State: Division of Corporations **Website:** https://icis.corp.delaware.gov/Ecorp/EntitySearch/NameSearch.aspx **Registration Number Format:** (State File Number) A 7-digit number. For example: 1234567

Revision History

Date	Detail
October 1, 2022	Updated agency search website for the California Secretary of State
December 9, 2021	Initial list including California and Delaware jurisdictions.

Appendix C - Registration Schemes for Organization Identifier in S/MIME Certificates

The following registration schemes are recognized as valid under this Apple Public CPS:

NTR:
For an identifier allocated by a national trade register to a Legal Entity named in the subject:organizationName.

VAT:
For an identifier allocated by the national tax authorities to a Legal Entity named in the subject:organizationName.

PSD:
For a national authorization number allocated to a payment service provider named in the subject:organizationName under Payments Services Directive (EU) 2015/2366. This shall use the extended structure as defined in ETSI TS 119 495 clause 5.2.1.

LEI:
For a global Legal Entity Identifier as specified in ISO 17442 for the entity named in the subject:organizationName. The 2 character ISO 3166 country code SHALL be set to 'XG'.

Appendix D - Revocation Reason Code Selection

This section applies to revocations that are performed after October 1, 2022. Revocation entries that appeared on a CRL prior to October 1, 2022, do not need to be changed.

The Apple Public CA supports the following revocation reason codes for Subscriber Certificates:

- unspecified
- keyCompromise
- affiliationChanged
- superseded
- cessationOfOperation
- privilegeWithdrawn

Reason Code Selection for Subscribers Requesting Revocation

Subscribers have access to the revocation reasons below through the revocation tools that the Apple Public CA provides. The Subscriber Representative requesting revocation must understand the revocation reason code and select the one that best matches the situation.

Reason Code	RFC 5280 reasonCode Value	Situations to Select Reason
unspecified	0	Represented by the omission of a reasonCode. Code is omitted unless the CRL entry is for a Subscriber Certificate subject to the CA/Browser Forum's Baseline Requirements revoked prior to July 15, 2023.
keyCompromise	1	Indicates that it is known or suspected that the Subscriber's Private Key has been compromised. For example, the Subscriber has lost control of, misplaced, or is aware of or suspects that unauthorized copies of the Private Key associated to the Public Key in the Certificate exist.
superseded	4	Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate for reasons such as endpoint/website/email address/ organization changed and the prior one will no longer be used.
cessationOfOperation	5	The endpoint/website/email address with the Certificate is shut down/discontinued prior to the expiration of the Certificate, or the Subscriber no longer owns, is authorized to use, controls one or more of the Domain Name(s), or email address in the Certificate.

Reason Code Selection for Apple Public CA

Unless the keyCompromise reason code is being used, Apple Public CA will select reason codes below based on the situation that best matches the situation.

Reason Code	RFC 5280 reasonCode Value	Situations to Select Reason
Unspecified	0	The Apple Public CA: • receives a written request, without specifying a CRLreason, from the Subscriber, • right to issue Certificates under this CPS expires or is revoked or terminated, unless the Apple Public CA has made arrangements to continue maintaining the CRL/ OCSP Repository, or • ascertains revocation is required by this CPS for a reason that is not otherwise required to be specified by Section 4.9.1.1 Selecting this reason results in no reasonCode CRL entry extension being provided in the CRL.
keyCompromise	1	The Subscriber has requested that their certificate be revoked for this reason; or The Apple Public CA: • obtains verifiable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a key compromise (See Section 4.9.12), • is made aware of a demonstrated or proven method that exposes the Private Key to compromise, • is made aware of clear evidence that the specific method used to generate the Private Key was flawed, or • is made aware of a demonstrated or proven method that can easily compute the Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/TLSkeys)
affiliationChanged	3	The Apple Public CA has replaced the Certificate due to changes in the Certificate's subject information (For example the name of the organization or jurisdiction has changed) and has not replaced the Certificate for the other reasons: keyCompromise, superseded, cessationOfOperation, or privilegeWithdrawn.

Reason Code	RFC 5280 reasonCode Value	Situations to Select Reason
superseded	4	The Subscriber has requested that their Certificate be revoked for this reason, or The Apple Public CA: • obtains reasonable evidence that the validation of domain authorization or control for any FQDN, IP address, or email address in the Certificate should not be relied upon, or • ascertains the Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 • becomes aware of compliance reasons such as the Certificate does not comply with an Application Software Supplier's policy, the CAB Forum's Baseline Requirements, or this CPS.
cessationOfOperation	5	The Subscriber has requested that their Certificate be revoked for this reason, or The Apple Public CA is made aware of: • any circumstance indicating that use of a FQDN, IP address, or email address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name), • the endpoint/website/email address with the Certificate is shut down prior to the expiration of the Certificate, or • the Subscriber no longer owns, is authorized to use, or controls one or more of the Domain Name(s) in the Certificate.

Reason Code	RFC 5280 reasonCode Value	Situations to Select Reason
priviledgeWithdrawn	9	The Apple Public CA: • obtains evidence that the Certificate was misused, • is made aware that the Subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use, • is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN, • is made aware of a material change in the information contained in the Certificate, • determines or is made aware that any of the information appearing in the Certificate is inaccurate, or • is made aware that the original Certificate Application was not authorized and that the Subscriber does not retroactively grant authorization.