Apple Inc.

Certification Practice Statement
Apple Public CA

Version 6.2.1

Effective Date: May 20, 2024

Table of Contents

1. INTRODUCTION 1
   1.1. OVERVIEW 1
   1.2. DOCUMENT NAME AND IDENTIFICATION 2
      1.2.1. Revisions 3
   1.3. PKI PARTICIPANTS 7
      1.3.1. Certification Authorities 7
      1.3.2. Registration Authorities 7
      1.3.3. Subscribers 8
      1.3.4. Relying Parties 8
      1.3.5. Other Participants 8
   1.4. CERTIFICATE USAGE 9
      1.4.1. Appropriate Certificate Uses 9
      1.4.2. Prohibited Certificate Uses 9
   1.5. POLICY ADMINISTRATION 9
      1.5.1. Organization Administering the Document 9
      1.5.2. Contact Person 9
      1.5.3. Person Determining CPS Suitability for the Policy 10
      1.5.4. CPS Approval Procedures 10
   1.6. DEFINITIONS AND ACRONYMS 10
      1.6.1. Definitions 10
      1.6.2. Acronyms 12
      1.6.3. References 13
      1.6.4. Conventions 14
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 15
   2.1. REPOSITORIES 15
   2.2. PUBLICATION OF CERTIFICATION INFORMATION 15
   2.3. TIME OR FREQUENCY OF PUBLICATION 15
   2.4. ACCESS CONTROLS ON REPOSITORIES 16
3. IDENTIFICATION AND AUTHENTICATION 17
   3.1. NAMING 17
      3.1.1. Types of Names 17
      3.1.2. Need for Names to be Meaningful 17
      3.1.3. Anonymity or Pseudonymity of Subscribers 17

3.1.4. Rules of Interpreting Various Name Forms 17
3.1.5. Uniqueness of Names 17
3.1.6. Recognition, Authentication, and Role of Trademarks 18
3.2. INITIAL IDENTITY VALIDATION 18
3.2.1. Method to Prove Possession of Private Key 18
3.2.2. Authentication of Organization Identity, Unique Domain Identity and Email Control 18
3.2.3. Authentication of Individual Identity 23
3.2.4. Non-Verified Subscriber Information 23
3.2.5. Validation of Authority 23
3.2.6. Criteria for Interoperation 24
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 25
3.3.1. Identification and Authentication for Routine Re-Key 25
3.3.2. Identification and Authentication for Re-Key After Revocation 25
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS 25
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 26
4.1. CERTIFICATE APPLICATION 26
4.1.1. Who Can Submit a Certificate Application 26
4.1.2. Enrollment Process and Responsibilities 26
4.2. CERTIFICATE APPLICATION PROCESSING 27
4.2.1. Performing Identification and Authentication Functions 27
4.2.2. Approval or Rejection of Certificate Applications 28
4.2.3. Time to Process Certificate Applications 28
4.3. CERTIFICATE ISSUANCE 29
4.3.1. CA Actions During Certificate Issuance 29
4.3.2. Notification To Subscriber by the CA of Issuance of Certificate 29
4.4. CERTIFICATE ACCEPTANCE 29
4.4.1. Conduct Constituting Certificate Acceptance 29
4.4.2. Publication of the Certificate by the CA 30
4.4.3. Notification of Certificate Issuance by the CA to Other Entities 30
4.5. KEY PAIR AND CERTIFICATE USAGE 30
4.5.1. Subscriber Private Key and Certificate Usage 30
4.5.2. Relying Party Public Key and Certificate Usage 30
4.6. CERTIFICATE RENEWAL 30
4.6.1. Circumstance for Certificate Renewal 30

4.6.2. Who May Request Renewal 30
4.6.3. Processing Certificate Renewal Requests 30
4.6.4. Notification of New Certificate Issuance to Subscriber 30
4.6.5. Conduct Constituting Acceptance of a Certificate Renewal 31
4.6.6. Publication of the Renewal Certificate by the CA 31
4.6.7. Notification of Certificate Issuance by the CA to Other Entities 31
4.7. CERTIFICATE RE-KEY 31
4.7.1. Circumstance for Certificate Re-Key 31
4.7.2. Who May Request Certification of a New Public Key 31
4.7.3. Processing Certificate Re-Keying Requests 31
4.7.4. Notification of New Certificate Issuance to Subscriber 31
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate 31
4.7.6. Publication of the Re-Keyed Certificate by the CA 31
4.7.1. Notification of Certificate Issuance by the CA to Other Entities. 31
4.8. CERTIFICATE MODIFICATION 31
4.8.1. Circumstance for Certificate Modification 32
4.8.2. Who May Request Certificate Modification 32
4.8.3. Processing Certificate Modification Requests 32
4.8.4. Notification of New Certificate Issuance to Subscriber 32
4.8.5. Conduct Constituting Acceptance of Modified Certificate 32
4.8.6. Publication of the Modified Certificate by the CA 32
4.8.7. Notification of Certificate Issuance by the CA to Other Entities 32
4.9. CERTIFICATE REVOCATION AND SUSPENSION 32
4.9.1. Circumstances for Revocation 32
4.9.2. Who Can Request Revocation 36
4.9.3. Procedure for Revocation Request 36
4.9.4. Revocation Request Grace Period 36
4.9.5. Time Within Which CA Must Process the Revocation Request 36
4.9.6. Revocation Checking Requirement for Relying Parties 37
4.9.7. CRL Issuance Frequency 37
4.9.8. Maximum Latency for CRLs 37
4.9.9. On-Line Revocation/Status Checking Availability 37
4.9.10. On-Line Revocation Checking Requirements 38
4.9.11. Other Forms of Revocation Advertisements Available 38

4.9.12. Special Requirements Related to Key Compromise 38
4.9.13. Circumstances for Suspension 39
4.9.14. Who Can Request Suspension 39
4.9.15. Procedure for Suspension Request 39
4.9.16. Limits on Suspension Period 39
4.10. CERTIFICATE STATUS SERVICES 39
4.10.1. Operational Characteristics 39
4.10.2. Service Availability 39
4.10.3. Operational Features 40
4.11. END OF SUBSCRIPTION 40
4.12. KEY ESCROW AND RECOVERY 40
4.12.1. Key Escrow and Recovery Policy and Practices 40
4.12.2. Session Key Encapsulation and Recovery Policy and Practices 40
5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS 41
5.1. PHYSICAL security CONTROLS 41
5.1.1. Site location and construction 41
5.1.2. Physical Access 41
5.1.3. Power and Air Conditioning 41
5.1.4. Water Exposures 41
5.1.5. Fire Prevention and Protection 41
5.1.6. Media Storage 42
5.1.7. Waste Disposal 42
5.1.8. Off-Site Backup 42
5.2. PROCEDURAL CONTROLS 42
5.2.1. Trusted Roles 42
5.2.2. Number of Persons Required per Task 43
5.2.3. Identification and Authentication for Each Role 43
5.2.4. Roles Requiring Separation of Duties 43
5.3. PERSONNEL CONTROLS 44
5.3.1. Qualifications, Experience, and Clearance Requirements 44
5.3.2. Background Check Procedures 44
5.3.3. Training Requirements 44
5.3.4. Retraining Frequency and Requirements 45
5.3.5. Job Rotation Frequency and Sequence 45

5.3.6. Sanctions for Unauthorized Actions 45
5.3.7. Independent Contractor Requirements 45
5.3.8. Documentation Supplied to Personnel 45
5.4. AUDIT LOGGING PROCEDURES 45
5.4.1. Types of Events Recorded 45
5.4.2. Frequency of Processing Log 46
5.4.3. Retention Period for Audit Log 47
5.4.4. Protection of Audit Log 47
5.4.5. Audit Log Backup Procedures 47
5.4.6. Audit Collection System (Internal Vs. External) 47
5.4.7. Notification To Event-Causing Subject 47
5.4.8. Vulnerability Assessments 47
5.5. RECORDS ARCHIVAL 48
5.5.1. Types of Records Archived 48
5.5.2. Retention Period for Archive 49
5.5.3. Protection of Archive 49
5.5.4. Archive Backup Procedures 49
5.5.5. Requirements for Time-Stamping of Records 49
5.5.6. Archive Collection System (Internal or External) 49
5.5.7. Procedures to Obtain and Verify Archive Information 49
5.6. KEY CHANGEOVER 50
5.7. COMPROMISE AND DISASTER RECOVERY 50
5.7.1. Incident and Compromise Handling Procedures 50
5.7.2. Computing Resources, Software, and/or Data Are Corrupted 50
5.7.3. Entity Private Key Compromise Procedures 51
5.7.4. Business Continuity Capabilities After a Disaster 51
5.8. CA OR RA TERMINATION 51
6. TECHNICAL SECURITY CONTROLS 52
6.1. KEY PAIR GENERATION AND INSTALLATION 52
6.1.1. Key Pair Generation 52
6.1.2. Private Key Delivery to Subscriber 53
6.1.3. Public Key Delivery to Certificate Issuer 53
6.1.4. CA Public Key Delivery to Relying Parties 53
6.1.5. Key Sizes 53

6.1.6. Public Key Parameters Generation and Quality Checking 54
6.1.7. Key Usage Purposes (as per X.509 v3. Key Usage Field) 54
6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 54
6.2.1. Cryptographic Module Standards and Controls 54
6.2.2. Private Key (n out of m) Multi-Person Control 54
6.2.3. Private Key Escrow 55
6.2.4. Private Key Backup 55
6.2.5. Private Key Archival 55
6.2.6. Private Key Transfer Into or From a Cryptographic Module 55
6.2.7. Private Key Storage on Cryptographic Module 55
6.2.8. Method of Activating Private Key 55
6.2.9. Method of Deactivating Private Key 55
6.2.10. Method of Destroying Private Key 56
6.2.11. Cryptographic Module Rating 56
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT 56
6.3.1. Public Key Archival 56
6.3.2. Certificate Operational Periods and Key Pair Usage Periods 56
6.4. ACTIVATION DATA 56
6.4.1. Activation Data Generation and Installation 56
6.4.2. Activation Data Protection 56
6.4.3. Other Aspects of Activation Data 56
6.5. COMPUTER SECURITY CONTROLS 57
6.5.1. Specific Computer Security Technical Requirements 57
6.5.2. Computer Security Rating 57
6.6. LIFE CYCLE TECHNICAL CONTROLS 57
6.6.1. System Development Controls 57
6.6.2. Security Management Controls 57
6.6.3. Life Cycle Security Controls 58
6.7. NETWORK SECURITY CONTROLS 58
6.8. TIME-STAMPING 58
7. CERTIFICATE, CRL, AND OCSP PROFILES 59
7.1. CERTIFICATE PROFILE 59
7.1.1. Version Numbers 59

7.1.2. Certificate Content and Extensions 59
7.1.3. Algorithm Object Identifiers 71
7.1.4. Name Forms 72
7.1.5. Name Constraints 76
7.1.6. Certificate Policy Object Identifier 76
7.1.7. Usage of Policy Constraints Extension 81
7.1.8. Policy Qualifiers Syntax and Semantics 81
7.1.9. Processing Semantics for the Critical Certificate Policies Extension 81
7.2. CRL PROFILE 81
7.2.1. Version Number 82
7.2.2. CRL and CRL Entry Extensions 82
7.3. OCSP PROFILE 83
7.3.1. Version Number 83
7.3.2. OCSP Extensions 84
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 85
8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 85
8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR 85
8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 85
8.4. TOPICS COVERED BY ASSESSMENT 85
8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY 85
8.6. COMMUNICATION OF RESULTS 86
8.7. SELF-AUDITS 86
8.8. Review of delegated parties 86
9. OTHER BUSINESS AND LEGAL MATTERS 87
9.1. FEES 87
9.1.1. Certificate Issuance or Renewal Fees 87
9.1.2. Certificate Access Fees 87
9.1.3. Revocation or Status Information Access Fees 87
9.1.4. Fees for Other Services 87
9.1.5. Refund Policy 87
9.2. FINANCIAL RESPONSIBILITY 87
9.2.1. Insurance Coverage 87
9.2.2. Other Assets 87
9.2.3. Insurance or Warranty Coverage for End-Entities 88

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION 88
9.3.1. Scope of Confidential Information 88
9.3.2. Information Not Within the Scope of Confidential Information 88
9.3.3. Responsibility To Protect Confidential Information 88
9.4. PRIVACY OF PERSONAL INFORMATION 88
9.4.1. Privacy Plan 88
9.4.2. Information Treated as Private 89
9.4.3. Information Not Deemed Private 89
9.4.4. Responsibility To Protect Private Information 89
9.4.5. Notice and Consent To Use Private Information 89
9.4.6. Disclosure Pursuant to Judicial or Administrative Process 89
9.4.7. Other Information Disclosure Circumstances 89
9.5. INTELLECTUAL PROPERTY RIGHTS 89
9.6. REPRESENTATIONS AND WARRANTIES 89
9.6.1. CA Representations and Warranties 89
9.6.2. RA Representations and Warranties 90
9.6.3. Subscriber Representations and Warranties 90
9.6.4. Relying Party Representations and Warranties 91
9.6.5. Representations and Warranties of Other Participants 92
9.7. DISCLAIMERS OF WARRANTIES 92
9.8. LIMITATIONS OF LIABILITY 92
9.9. INDEMNITIES 94
9.9.1. Indemnification by Apple 94
9.9.2. indemnification By Subscribers 94
9.9.3. Indemnification By Relying Parties 94
9.10. TERM AND TERMINATION 95
9.10.1. Term 95
9.10.2. Termination 95
9.10.3. Effect of Termination and Survival 95
9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 95
9.12. AMENDMENTS 95
9.12.1. Procedure for Amendment 95
9.12.2. Notification Mechanism and Period 96
9.12.3. Circumstances Under Which OID Must Be Changed 96

9.13. DISPUTE RESOLUTION PROVISIONS 96
9.14. GOVERNING LAW 96
9.15. COMPLIANCE WITH APPLICABLE LAW 96
9.16. MISCELLANEOUS PROVISIONS 96
9.16.1. Entire Agreement 96
9.16.2. Assignment 96
9.16.3. Severability 97
9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights) 97
9.16.5. Force Majeure 97
9.17. OTHER PROVISIONS 97
Appendix A: Apple Subordinate CAs Hierarchy 98
Appendix B: Verification Sources 100
Sources List 100
Revision History 100
Appendix C: Registration Schemes for Organization Identifier in S/MIME Certificates ..101
Appendix D: Revocation Reason Code Selection 102

1. INTRODUCTION

1.1. OVERVIEW

This Certification Practice Statement ("CPS") describes the practices employed by Apple Inc. acting as a publicly-trusted Certification Authority ("Apple Public CA") in issuing and managing digital Certificates and related services to:

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

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. Apple Public CA issues Certificates for Apple Inc. and its subsidiaries.

The Apple Public CA is issued Certificates by publicly-trusted Root Certification Authorities ("Root CA") that are widely trusted by suppliers of Internet browser software or other relying-party application software. As such, the Apple Public CA inherits the benefits and responsibilities associated with the public trust from the issuing public Root CAs. Appendix A lists all valid Subordinate CA Certificates ("Sub-CA Certificate") issued to Apple Public CA by Root CAs.

This CPS provides all the practices for issuance of Organization Validated ("OV") and Extended Validation ("EV") TLS Server Certificates, and Mailbox-validated and Organization-validated S/MIME Certificates. Any practice that is designed for a specific Certificate type is explicitly identified.

This CPS meets the current versions of the following policies, guidelines, and requirements:

Name of Policy/ Guideline/ Requirement Standard	Location of Source Document
The Certification Authority / Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")	https://cabforum.org/baseline-requirements-documents/
The Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates ("S/MIME Baseline Requirements")	https://cabforum.org/smime-br/
The CAB Forum Guidelines For The Issuance And Management Of Extended Validation Certificates ("EV Guidelines")	https://cabforum.org/extended-validation/

Name of Policy/ Guideline/ Requirement Standard	Location of Source Document
The CAB Forum Network and Certificate System Security Requirements	https://cabforum.org/network-security-requirements/
Apple Root Store Program	https://www.apple.com/certificateauthority/ca_program.html
Chromium Root Store Policy	https://www.chromium.org/Home/chromium-security/root-ca-policy
Microsoft Root Certificate Program	https://docs.microsoft.com/en-us/security/trusted-root/program-requirements
Mozilla Root Store Policy	https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
Oracle Java	https://www.oracle.com/technetwork/java/javase/javasecarootcertsprogram-1876540.html

The presence of a CAB Forum Reserved Certificate Policy Identifier, in Section 7.1.6.1.1, asserts that Apple makes commercially reasonable efforts to conform to the latest version of the CAB Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates and the CAB Forum Guidelines For The Issuance And Management Of Extended Validation Certificates published at http://www.cabforum.org. In the event of any inconsistency between this CPS and the CAB Forum Requirements, they will take precedence over this CPS.

1.2. DOCUMENT NAME AND IDENTIFICATION

This is the Apple Public CA CPS. The name reflects the publicly-trusted nature of the Certification Authority regulated by this CPS, and supersedes the prior name "Apple IST CPS".

The Apple Public CA designated the applePublicPolicyID arc to identify objects such as documents and Certificates within the PKI:

{iso(1) member-body(2)
us(840)
apple(113635)
appleDataSecurity(100)
appleDocument(20)
applePKIPolicyDocument(1)
applePKICertificationPracticeStatements(2)
applePublicCPS(2)}
(1.2.840.113635.100.20.1.2.2)

Certificate Policy identifiers that have been reserved for use by Apple Public CA to assert compliance are documented in Section 7.1.6.1

1.2.1. Revisions

The Apple Public CA CPS is reviewed and updated at least annually, as required by the Baseline Requirements. It is structured according to RFC3647; the words "No stipulation" are applied to section headings if the Apple Public CA imposes no requirements related to that section.

The following revisions have been made to the original document:

Date	Changes	Version
05/20/2024	Updated following sections to remove practices around Certificate renewal, standardized Key Operation Periods and Certificate validity for S/MIME Certificates. Introduced a new Apple Reserved Policy OID to be used in some S/MIME Certificates. Sections include: 3.3.1, 4.3.1, 4.6, 4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7, 6.1.3, 6.3.2, 7.1.2 and 7.1.6. Generalized Certificate Problem Report practices in Section 1.5.2.1.	6.2.1
03/15/2024	Updated multiple sections to bring the document to compliance with Baseline Requirements up to version 2.0.2. including: 1.6.3, 4.9.7, 4.9.9, 4.9.10, 7.1.2.7, 7.1.2.8, 7.1.2.11, 7.2, 7.2.1, 7.2.2, and Appendix D. Updated Appendix A to remove two revoked subCAs and added two new subCAs. Updated self-audit practices for SMIME Certificates in Section 8.7. Made editorial updates in Sections 1.3.3, 1.6.1, 1.6.2, 3.1.2, 3.1.3, 5.1, 6.2.8 and 7.3.1. Multiple other Sections updated for TLS Server Certificates.	6.2
01/30/2024	Updated multiple sections to address new practices for removal of recurrent background checks and use of new Commit Signing policy OIDs to indicate use of hardware. Section 5.3.2 removes recurrent 5-year background checks. Sections 7.1.2.7, 7.1.6.1.2 and 7.1.6.1.3 adds Commit Signing policy OIDs and corresponding use in profiles Sections 6.2.1, 6.2.7 and 6.2.8 adds practices for use of hardware Cryptographic Modules and interaction with system.	6.1
09/14/2023	Updated Sections 1.1, 1.3.2.1, 1.3.5, 1.4.1.2, 1.6.1, 1.6.2, 3.1.5, 3.2.2.1, 3.2.5, 3.2.6, 3.3.1, 4.6, 4.6.1, 4.9.1.1, 4.9.2, 4.9.3, 6.3.2, 7.1.2.7, 7.1.2.10, 7.1.4.2, 7.1.4.3, 7.1.6.1, 7.1.6.3 and 8.8 for editorial and clarification updates.	6.0.1
09/01/2023	Updated multiple sections to bring the document to compliance with Baseline Requirements up to version 2.0., S/MIME Baseline Requirements up to version 1.0.1 and EV Guidelines up to version 1.8.0	6.0

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 - changed business day for calendar days. Section 3.2.5 - established the connection between Reliable Communication Methods and authority validation. 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 4.9.3 - 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. Section 5.7.1 - updated text clarify meaning of practices related to reporting. Section 6.1.1.1 - updated the ceremony's video recording practice.	5.11
10/01/2022	Updated Sections 1.6.1, 1.6.2, 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 Sections 4.9.1.1 and 9.6.3.	5.10
09/01/2022	Updated Sections 3.2.2.4, 3.2.2.8, 5.4.1, 5.4.2, 5.4.3, 5.4.6, 5.5.1, and 5.5.2 for compliance with CABF Baseline Requirements from versions 1.8.3 and 1.8.4. Updated Section 5.5.7 and 9.10 to simplify text and correct section numbering. Updated Section 9.14 to change governing law.	5.9
07/25/2022	Updated section 4.9.7 to simplify CRL issuance frequency language, Section 5.1.4 to better reflect water protection practices in diverse facilities, and Section 7.1.2 to support use cases for TLS Server Certificates with client authentication.	5.8
06/16/2022	Updated Sections 4.9.7 and 4.9.8 to better reflect practices associated to CRL configurations.	5.7

Date	Changes	Version
04/30/2022	Updated Section 4.1.1. to ensure compliance with the Baseline Requirements up to version 1.8.2. Updated Sections 1.2, 1.6, 3.1.2, 3.1.5, 3.2.2, 3.2.2.1, 3.2.2.9, 3.2.2.10, 3.2.5, 4.1.1, 4.1.2.1, 6.1.1.3, 6.1.2, 7.1.2, 7.1.4.2 and added Appendix C to include Mailbox-Validated and Sponsor-Validated S/MIME certificates-related practices. Updated Appendix A to record two new subCAs. Updated Sections 5.2.1.4, 5.2.2 and 5.3.7 to expand certain Trusted Roles to contractors. Updated legal aspects in Sections 3.1.6 , 9.4.1–9.4.7, 9.5, 9.6.3, 9.8, 9.9.3, 9.11, 9.15, and 9.16.2. Updated Sections 3.2.2.6, 3.2.2.10, 5.1.1., 5.1.8, 5.4.5, 5.4.6, 5.5.1, 5.5.2, 5.5.4 and 5.7.1 for minor errata.	5.6
10/21/2021	Updated Section 4.12.1 to clarify key recovery process. Updated Section 7.1.2 to schedule removal of Key Agreement from TLS Server Certificates.	5.5
10/01/2021	Updated Sections 3.2.2.4, 3.2.6, 4.9.1.1, 7.1.2, 7.1.4.2. and 7.1.4.3 to ensure compliance with the Baseline Requirements up to version 1.8.0 and EV Guidelines up to version 1.7.8.	5.4
08/26/2021	Updated Section 4.2.1, to ensure compliance with the Baseline Requirements up to version 1.7.8. Updated Section 4.2.1 to ensure compliance with EV Guidelines up to version 1.7.6. Minor text changes to tables in Section 7.1.2 to increase accuracy of descriptions. Updated Appendix A to include a new sub-CA Certificate.	5.3
04/30/2021	Updated multiple sections to ensure compliance with the Baseline Requirements up to version 1.7.4, EV Guidelines version 1.7.5 and Network and Certificates System Security Requirements up to version 1.7. Updated Sections 4.2.1, 4.9.12, 8.1, 8.2, 8.6 and 9.11 to meet new requirements from Mozilla Root Store Policy version 2.7.1. Updated Sections 5.3.1, 5.3.2 and 5.3.3 to modernize background check practices. Made editorial and clarification updates in multiple sections.	5.2

Date	Changes	Version
09/24/2020	Updated the document to ensure compliance with the Baseline Requirements up to version 1.7.1 and EV Guidelines version 1.7.3. Made minor grammatical updates.	5.1
04/29/2020	Updated the document to include practices for issuance of EV Certificates compliant with the "Guidelines For The Issuance And Management Of Extended Validation Certificates".	5.0
04/01/2020	Updated the document to meet requirements of version 2.7 of the Mozilla Root Store Policy. Completed annual review as required by the Baseline Requirements. Incorporated content from the Apple Corporate Email CPS version 2.3 dated 06/05/2019.	4.3
06/14/2019	Updated contact information in Section 1.5.2 and made minor changes to Section 4.1.1 and 4.9.2.	4.2
05/31/2019	Removed deprecated Domain Authorization validation method in Section 3.2.2.1.	4.1
12/11/2018	Modified Section 1.1 to introduce the concept of Apple Public CA and removed references to Apple IST CA throughout the document. Modified Section 1.2 to introduce a new document name. Added the Organization Validated optional policy object identifier from the Baseline Requirements. Updated contact information in Section 1.5.2. Added Section 3.1.1.2 to include a new Sub-CA Certificate naming schema valid starting on December 11, 2018. Added Section 3.2.2.1 to specify the methods used for validation of authorization of control.	4.0
03/01/2018	Updated Section 6.3.2 to conform with CAB Forum ballot 193 – 825-day Certificate Lifetimes. Added definition for Certificate Transparency, and CT and TLS acronyms in Section 1.6. Added the SCT extension to profiles in Section 7.1.	3.4

Date	Changes	Version
09/06/2017	Removed reference to IST CA 6 in Section 1.1. Updated definitions and acronyms in Section 1.6 to include CAA. Updated Section 4.2.1 to conform with CAB Forum ballot 187 - Make CAA Checking Mandatory. Updated font to SF Hello Thin. Updated references of WebTrust governing body to CPA Canada.	3.3
12/01/2016	Added references to the specific CAs covered in the CPS: IST CA 3, and IST CA 6.	3.2
08/15/2016	Added references to the specific CAs covered in the CPS: IST CA 2, IST CA 4, and IST CA 8.	3.1
01/28/2016	Updates to clarify that CAA records are not reviewed. Clarifications on the scope of cryptographic module engineering controls. Minor grammatical updates.	3.0
02/16/2015	Updates for conformance with SSL Baseline Requirements for Publicly Trusted Certificates.	2.0
08/25/2014	Initial release.	1.0

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

This is an entity that is authorized to issue, manage, and revoke Certificates. Apple Public CA acts as the Certification Authority.

1.3.2. Registration Authorities

The Registration Authority performs identification and authentication checks for end-user Certificate applicants. Apple Public CA acts as the 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

This is an entity who has been issued a Certificate signed by an Apple Public CA Certificate. 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

This is any entity that receives a Certificate (issued to a Subscriber by the Apple Public CA) and has an interest of some kind in the validity of the Certificate.

1.3.5. Other Participants

1.3.5.1. CAB Forum

The CAB Forum is a voluntary organization of CAs and suppliers of Internet browser and other relying-party software applications.

1.3.5.2. Application Software Supplier

A supplier of Internet browser software or other relying party application software that displays or uses Certificates and incorporates Root Certificates.

1.3.5.3. Root Certificate Authority

A Root CA is a top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Sub-CA Certificates. Apple Public CA has established relationships with Root CAs to obtain Sub-CA Certificates used for the issuance of publicly-trusted TLS and S/MIME Certificates.

1.3.5.4. Apple CA Policy Authority

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 optional 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. Email messages signed with an S/MIME Certificate are not intended to replace a written or electronic signature. These S/MIME Certificates are only intended to indicate that the email message is from an authorized email account, and do not provide any assurance of the identity of the sending party.

S/MIME Certificates that include the Apple-owned Commit Signing purpose, in addition to the Email Protection purpose, can be used to sign changes made to a git repository.

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 Apple CA Policy Authority.

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 may contact us by following instructions at 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 Apple CA Policy Authority determines the suitability and applicability of this CPS. The Apple CA Policy Authority shall consider, among other factors, the results and observations received from independent auditors as specified in Section 8, as well as recommendations from Root CAs with relationships with the Apple Public CA, internal auditors, and Application Software Suppliers.

1.5.4. CPS Approval Procedures

This CPS and all amendments to this CPS are subject to approval by the Apple CA Policy Authority. 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 History as specified 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 CAB Forum definitions in the Baseline Requirements, the S/MIME Baseline Requirements, the Network and Certificate System Security Requirements, and the EV Guidelines.

Some terms that are not defined by the CAB Forum, or need to be expanded within the Apple Public CA's context, are included in the table below.

This section describes the general meaning of these terms as used.

Term	Definition
Certificate Application	The document, physical or electronic, submitted by a Subscriber to Apple Public CA for the purpose of obtaining a Certificate. An EV Certificate Request is a Certificate Application for an EV Certificate.

Term	Definition
Certificate Chain	This is a collection of Certificates that are considered as a group to verify the authenticity of a particular Certificate. In the usual X.509 certificate model, the Certificate to be verified issued by a Sub-CA to a Subscriber. The Certificate for the Sub-CA is in turn signed by the Root CA Certificate. Each issued Certificate contains a digital signature signed by its issuer. The digital signature can be verified at the request of a Relying Party by both the Sub-CA and Root CA so as to authenticate the source and integrity of the Certificates and any objects signed or encrypted using the related Public/Private Keys.
Certificate Transparency	A protocol for publicly logging the existence of TLS Server Certificates as they are issued or observed, in a manner that allows anyone to audit Certificate Authority activity and notice the issuance of suspect Certificates as well as to audit the Certificate logs themselves.
Common CA Database (CCADB)	The Common CA Database is a repository of information about externally operated CAs whose Root and Subordinate Certificates are included within the products and services of Application Software Supplier that are CCADB members. Application Software Suppliers participate in the CCADB to improve security, transparency, and interoperability (See https://www.ccadb.org).
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.
Internationalized Domain Name	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).
Precertificate	A cryptographic object that is constructed from the Certificate to be issued by adding a special critical poison extension (OID 1.3.6.1.4.1.11129.2.4.3, and extnValue NULL) to the end-entity TBSCertificate and signing the resulting TBSCertificate [RFC5280] with either: • a special-purpose (CA:true, Extended Key Usage: Certificate Transparency, OID 1.3.6.1.4.1.11129.2.4.4) Precertificate signing certificate. The Precertificate signing certificate MUST be directly certified by the (Root CA or Sub-CA) Certificate that will ultimately sign the end-entity TBSCertificate yielding the end-entity Certificate, or, • the Sub-CA Certificate that will sign the final certificate.
Repository	See Section 2.1
S/MIME	Secure/Multipurpose Internet Mail Extensions ("S/MIME") is a widely accepted standard for sending digitally signed and encrypted messages. See RFC5751 for further details.

1.6.2. Acronyms

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

Acronym	Term
CA	Certification Authority
CAA	Certification Authority Authorization
CAMT	Certification Authority Management Team
CCADB	Common CA Database
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
HSE	High Security Environment
IDN	Internationalized Domain Name
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Apple CA Policy Authority
PKI	Public Key Infrastructure
QGIS	Qualified Government Information Source
QTIS	Qualified Tax Information Source
RA	Registration Authority
Root CA	Root Certification Authority
Sub-CA	Subordinate Certification Authority
S/MIME	Secure/Multipurpose Internet Mail Extensions

Acronym	Term
TLS	Transport Layer Security
URL	Uniform Resource Locator

1.6.3. References

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

FIPS 140-3, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, March 22, 2019.

FIPS 186-4, Federal Information Processing Standards Publication - Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology, July 2013.

ISO 17442-1:2020, Financial services — Legal entity identifier (LEI) - Part 1: Assignment.

ISO 17442-2:2020, Financial services — Legal entity identifier (LEI) - Part 2: Application in digital certificates.

Network and Certificate System Security Requirements, Version 1.7 or later. See https://cabforum.org/network-security-requirements/.

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework. S. Chokhani, et al. November 2003.

RFC3912, Request for Comments: 3912, WHOIS Protocol Specification. L. Daigle. September 2004.

RFC 4262, Request for Comments: 4262, X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities, S. Santesson. December 2005.

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile. D. Cooper, et al. May 2008.

RFC 6818, Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. January 2013.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. S. Santesson, et al. June 2013.

RFC6962, Request for Comments: 6962, Certificate Transparency. B. Laurie, et al. June 2013.

RFC 8398, Request for Comments: 8398, Internationalized Email Addresses in X.509 Certificates, MAY 2018. A. Melnikov, et al. May 2018.

RFC 8499, Request for Comments: 8499, DNS Terminology. P. Hoffman, et al. January 2019.

RFC8659, Request for Comments: 8659, DNS Certification Authority Authorization (CAA) Resource Record, P. Hallam-Baker, et al. November 2019.

RFC8954, Request for Comments: 8954, Online Certificate Status Protocol (OCSP) Nonce Extension. M. Sahni, Ed. November 2020.

X.509, Recommendation ITU-T X.509 (08/2005) | ISO/IEC 9594-8:2005, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute Certificate frameworks.

WebTrust for Certification Authorities, SSL Baseline with Network Security, available at https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

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.

CAB Forum Requirement’s effective dates will be translated to Pacific Standard Time or Pacific Daylight Savings, as appropriate, to account for the timezone differences.

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.
- Sub-CA Certificates and status information for Subscriber Certificates are available from publicly accessible locations linked from the Subscriber Certificate.
- The current version, and previous versions of, 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 version of this CPS and agreements are published at www.apple.com/certificateauthority/public or www.apple.com/certificateauthority and are readily accessible on a 24x7 basis.

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

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 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

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, the EV Guidelines, 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.

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

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.

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 Distinguished Name ("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") included in the Subject Alternative Name extension and Common Name field identify the device(s) controlled by the Subscriber. For IDNs, Apple Public CA may include the Punycode version of the IDN.

S/MIME 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, and the verified Mailbox Address; 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, 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 (e.g. ó for o, ñ for n, ç for c). 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
TLS Server Certificate	Inclusion of the Domain Name in the Certificate. Domain name 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").

For S/MIME Certificates that include the Commit Signing purpose in the Extended Key Usage, the Certificate Applicant must demonstrate possession of the Private Key corresponding to the Public Key listed in the Certificate by establishing a successful mutual TLS authentication session to the enrollment system using its Identification Credential. The Public Key in the Identification Credential is included in the Commit Signing Certificate.

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 where the Applicant is a Legal Entity, 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 organizational unit of 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 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

Apple Public CA verifies the Applicant's 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:

- A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition as listed in Appendix B, or
- A site visit by a representative of the Apple Public CA, or
- An Attestation Letter provided by the Applicant, or
- (Only for Organization-validated S/MIME Certificates) A Legal Entity Identifier (LEI) data reference. When an 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.

EV Certificates

Apple Public CA verifies the Applicant's existence and identity in accordance with the EV Guidelines. Specifically, the legal existence and identity, physical existence, and operational existence, are verified through the one of these methods:

- Use of a QGIS operated by, or on behalf of, the incorporating or registration agencies in the Applicant's jurisdiction as listed in Appendix B, or
- Use of a Verified Professional Letter provided by the Applicant.

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

TLS Server Certificates and Organization-Validated S/MIME Certificates

When the Subject Identity Information includes a DBA or trademark, Apple Public CA uses a method described in Baseline Requirements Section 3.2.2.2 or S/MIME Baseline Requirements Section 3.2.3.2.2 to perform the verification of the specific type.

EV Certificates

Apple Public CA verifies the DBA information in accordance with the EV Guidelines using one of these methods:

- Use of QGIS operated by, or on behalf of, the incorporating or registration agencies in the Applicant's jurisdiction, or
- Use of a Verified Professional Letter provided by the Applicant.

3.2.2.3. Verification of Country

Apple Public CA includes countryName in all Certificates, which are verified in accordance with Section 3.2.2.1.

3.2.2.4. Validation of Domain Authorization or Control

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

Validation of FQDNs is performed using the 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.
- (3.2.2.4.7) – DNS Change, by confirming the presence of Random Value in either a DNS TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a Domain Label that begins with an underscore character. Confirmation is completed within 20 days of generation of the Random Value.

FQDNs are also reviewed to prevent use of Internal Names.

Apple Public CA does not issue Certificates with FQDNs that include Onion Domain Names or with mixed character sets.

3.2.2.5. Authentication for an IP address

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.

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

Apple Public CA verifies the Verified Professional Letter provided by the Applicant in accordance with the EV Guidelines Sections 11.11.1 and 11.11.2.

Apple Public CA verifies an Independent Confirmation from the Applicant in accordance with the EV Guidelines Sections 11.11.4.

The Independent Confirmation method relies on using a Verified Method of Communication for the Applicant. Verifying that the Method of Communication belongs to the Applicant is done through the use of:

- QGIS or QTIS, and/or
- Verified Professional Letter.

3.2.2.8. CAA Records

Prior to issuing a TLS Server Certificate, the Apple Public CA retrieves and processes the CAA record to verify the presence of "pki.apple.com" in either the 'issue' or 'issuewild' properties for each FQDN provided. The 'iodef' property is checked but no action will be taken. The following criteria will be used to establish whether to issue the Certificate:

- If the CAA record is not present in DNS, the Certificate will be issued.
- If the 'issue' and 'issuewild' properties are empty or list the name "pki.apple.com" as an authorized CA, the Certificate will be issued.
- If the 'issue' or 'issuewild' properties list a name other than "pki.apple.com" as an authorized CA, the Certificate will not be issued.
- In any other cases, the Certificate will not be issued.

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.

Apple Public CA logs actions taken based on CAA records, and documents issuance prevented by CAA for feedback to the CA/Browser 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 (For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate), 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. 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 in the request is compared to an externally compiled database of the top 1,000 most popular Domain Names. If any Base Domain is present in the list, and it is not owned/controlled by the Applicant, the request is rejected.

In addition, Apple Public CA's risk-mitigation criteria identify requests containing Wildcard Domain Names as high risk, so they are subject to a manual approval process.

3.2.2.11. Organization Unit Validation

For TLS Server Certificates, Apple Public CA prevents an Organization Unit attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity by including predefined strings that represent internal sub organizations. The pre-defined strings are pre-approved by Certificate Approvers and do not contain any names.

3.2.3. Authentication of Individual Identity

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

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

3.2.4. Non-Verified Subscriber Information

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 3.2.2.1.

TLS Server Certificates

The Apple Public CA will take reasonable steps to establish that a Certificate Application is from Apple staff. Certificate Requestors authenticate to the enrollment system with the Identification Credential that verifies they are an employee of the Subscriber, i.e., Apple Inc., before a Certificate Application can be submitted. A list of pre-approved Certificate Requestors, and their Identification Credentials, is included in the enrollment system.

EV Certificates and Organization-Validated S/MIME Certificates

Apple Public CA verifies the name, title and agency for Contract Signers and Certificate Approvers; the Contract Signer's Signing Authority and signature on the

Terms of Use; and the Certificate Approver's authority (both EV Authority and authority for Organization-validated S/MIME Certificates) using a combination of these methods:

- Verified Professional Letter. The letter is used to verify:
  - Contract Signer's name, title, agency, and Signing Authority
  - Certificate Approvers' name, title, agency, and authority
- Independent Confirmation from Applicant. The confirmation is used to verify:
  - Contract Signer's name, title, agency, and Signing Authority
  - Certificate Approvers' name, title, agency, and authority
- Contract Signer's Representation/Warranty. The representation is used to verify:
  - Contract and Signing Authority
  - Terms of Use's signature.

If it is necessary to verify the Contract Signer's signature because they have not been pre-authorized in accordance with EV Guidelines Section 11.8.4, the signature is verified in accordance with Section 11.9.2(1,3)

After the Contract Signer's authority is verified, they sign an agreement to expressly authorize one or more Certificate Approvers to exercise authority for future EV Certificate Requests and Organization-validated S/MIME certificate requests . A list of approved Certificate Approvers, and their Identification Credentials, is included in the enrollment system.

Certificate Approvers explicitly approve each EV Certificate Request. Apple Public CA requires the Certificate Approvers to present their Identification Credential before they can access the enrollment system to approve a pending EV Certificate Request.

Apple Public CA confirms that the Contract Signer and Certificate Approvers are not on any United States Government denied list, list of prohibited persons, or other list that prohibits doing business with such individuals.

Mailbox-Validated S/MIME Certificates

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

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

The Apple Public CA does not provide re-key services 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

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.

Only pre-authorized Certificate Requestors can submit EV Certificate Requests. Every EV Certificate Request is approved by an authorized Certificate Approver.

Apple Public CA will not issue EV Certificates to an Applicant if either the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Business is on any United States Government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person.

4.1.2. Enrollment Process and Responsibilities

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

- An executed 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 (for TLS Server Certificates) or the Applicants themselves (for S/MIME Certificates).

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

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, Contract Signer and Certificate 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 (e.g., QGIS). When documentation is not available in English, Apple Public CA will engage a translator.

TLS Server Certificates

- Applicant Identity: Sections 3.2.2.1, 3.2.2.2 and 3.2.2.3,
- Validation of Organization Unit: Section 3.2.2.11,
- 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 3.2.2.9, and
- Wildcard Domain Validation for TLS Server Certificates, other than EV: Section 3.2.2.6.

S/MIME Certificates

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

Age of Validated Data

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 existence and identity: 397 days
- Assumed name: 397 days
- Address of Place of Business: 397 days

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

Domain Name validation information for EV Certificates is used for the period mentioned above as long as the registrant remains the same between the original validation and the results of a WHOIS check performed before the EV Certificate Request is approved. Apple Public CA implements an automated and continuous check that triggers an alert when a registrant change occurs.

4.2.2. Approval or Rejection of Certificate Applications

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,
- are for a Mailbox Address associated to a Domain Name not owned/controlled by an authorized Applicant,
- are submitted by Certificate Requestors, or approved by a Certificate Approver, without proper authority, and
- remain incomplete or inconsistent after a reasonable amount of time after clarifications have been requested.

Approval of an EV Certificate Request requires the actions of two separate Validation Specialists, working on separate teams within the Apple Public CA that do not share those individuals. The first Validation Specialist verifies all the information about the Applicant, Contract Signer, Certificate Approvers, and Domain Names. The second Validation Specialist confirms the approval by the Certificate Approver, corroborates consistency of all other validations, and provides final approval. Only EV Certificate Requests with complete verifications and no inconsistent information will be approved.

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.

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, or in the Identification Credential for certain S/MIME Certificates,
- 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 Names 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,
- confirm that the Certificate has no missing or incorrect extensions and the Public Keys meet the parameters required in Section 6.1.6.

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. Apple Public CA may also record issuance of TLS Server Certificates to Certificate Transparency logs.

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

The Apple Public CA may notify 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.

4.5.2. Relying Party Public Key and Certificate Usage

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

Any warranties provided by 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 means the issuance of a new Certificate to the Subscriber with the same Public Key and verified information (e.g. identity, domains, Mailbox 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.

The Apple Public CA does not currently provide Certificate renewal.

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 Certificate Renewal

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 means 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 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 CRLreason, 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), or

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.

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 the Baseline Requirements or any section of the Mozilla Root Store policy,

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 Baseline Requirements 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 Baseline Requirements 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 governing CP and/or the CPS, or
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.

S/MIME Certificates

The Apple Public CA will revoke an 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 the Apple Public CA's 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 Certificate was issued in violation of the then-current version of the Mozilla Root Store Policy requirements.

4.9.1.2. Reasons for Revoking a Sub-CA Certificate

Apple Public CA may request revocation of a Sub-CA Certificate by its Root CA provider for one of the following reasons:

1. The original request for the Sub-CA Certificate was not authorized,

2. The Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Baseline Requirements Sections 6.1.5 and 6.1.6,

3. Apple Public CA determines that any of the information appearing in the Certificate is inaccurate or misleading,

4. Apple Public CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate, or

5. 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.

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 Apple Public CA of reasonable cause to revoke the Certificate.

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

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.

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, a revocation is required, 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 the revocation of an Apple Public CA Sub-CA Certificate chaining up to a root in Mozilla's root program is due to a security concern, Apple Public CA will work with its Root CA provider to revoke the Certificate and file an appropriate public disclosure.

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 Certificate Requestor and/or Certificate Approver associated to the Certificate. Reports to the Subscriber are submitted to the email associated to the original Certificate Application.

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. Apple Public CA provides revocation status via mechanisms that are embedded in the Certificate (e.g., CRL Distribution Point or OCSP pointer).

4.9.7. CRL Issuance Frequency

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.

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

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

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 URL noted in the Authority Information Access extension in the Certificate.

Apple Public CA provides URLs for all CRLs signed by its Sub-CA Certificates to each Root CA provider, in an appropriately-formatted structure (e.g., JSON Array), before any Subscriber Certificates are issued. Subsequent URL publication to the CCADB is carried out by each Root CA provider 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.

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.

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.

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 Related to Key Compromise

In the event of key compromise of the Sub-CA's Private Key, 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, 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 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 key reuse, effectively blocking 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

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.

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. Representatives of the organization named in the Certificate may obtain an escrowed Private Key after they demonstrate they have been authorized by the organization'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

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, Sub-CA Private Keys, which are stored in encrypted form, are moved to secure storage under dual control or by using secure transport methods recommended by the vendor. 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 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 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 the assignment of Issuing CAs and Certificate Profiles.

5.2.2. Number of Persons Required per Task

At least two individuals in Trusted Roles (both CA Administrators) are required for sensitive tasks, such as backing up and generating Sub-CA Private Keys.

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 must identify and authenticate themselves using multi-factor authentication before they are allowed access to the systems necessary to perform their Trusted Roles. CA Administrators require additional authentication to perform sensitive tasks such as backing up and generating Sub-CA Private Keys.

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.

EV Certificates

Apple Public CA enforces rigorous control procedures for separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate. These control procedures are auditable by means of system logs and validation artifacts. Systems used to process and approve EV Certificate Requests require actions by at least two individuals in Trusted Roles before creating an EV Certificate.

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 Person 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.

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.

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

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),
- CA/Browser Forum Baseline Requirements and EV Guidelines, and
- Applicable functions relative to their assigned Trusted Role.

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

EV Certificates

Personnel performing EV Certificate Validation must meet all above training requirements. The required examination also addresses the EV Certificate validation criteria in Section 3.2.

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:

- Sub-CA key lifecycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction, and
  - Cryptographic device lifecycle management events.
- Subscriber Certificate lifecycle management events, including:
  - Certificate Applications and revocation,
  - All verification activities stipulated in this CPS,
  - Approval and rejection of Certificate Applications and revocation requests,
  - Issuance of Certificates,
  - Generation of Certificate Revocation Lists, and
  - Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).
- Security events, including:
  - Successful and unsuccessful PKI system access attempts,
  - PKI and security system actions performed,
  - Security profile changes,
  - Installation, update and removal of software on a Certificate System,
  - System crashes, hardware failures, and other anomalies,
  - Firewall and router activities, and
  - Entries to and exits from the CA facility.

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

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

5.4.2. Frequency of Processing Log

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 Log

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

For Sub-CA key lifecycle management events, after the later occurrence of:

- The destruction of the CA Private Key, or
- 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.

For Subscriber Certificate lifecycle management events, after the expiration of the Subscriber Certificate.

For security events, 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 facilities, as defined in Section 5.4.5.

5.4.7. Notification To Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

Apple Public CA performs an annual risk assessment to:

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

- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes, and
- Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the Apple Public CA has in place to counter such threats.

5.5. RECORDS ARCHIVAL

5.5.1. Types of Records Archived

The Apple Public CA and Enterprise RAs archive the following types of records:

- Records of the events listed in Section 5.4.1,
- Known and suspected violations of physical security and, if applicable, remedial actions taken as a result,
- All versions of this CPS,
- Contracts and agreements (e.g., Relying Party Agreement, Subscriber Agreement, Terms of Use),
- System and equipment configurations, modifications, and updates,
- Sufficient identity authentication data to satisfy the identification requirements of Section 3.2,
- Issued Certificates,
- Data and applications necessary to verify the archive contents,
- Compliance auditor reports,
- Changes to audit parameters,
- Attempts to delete or modify audit logs,
- Access to Private Keys for key recovery purposes (S/MIME Certificates only),
- Export of Private Keys,
- Appointment of an individual to a Trusted Role,
- Destruction of a cryptographic module,
- All Certificate compromise notification requests,
- Certificate Problem Reports,
- Remedial action taken as a result of violations of physical security, and

- 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 and Enterprise RAs also retain 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

Apple Public CA archives are backed up to storage located 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 timestamps archive records as they are created. Cryptographic time-stamping of archive records is not required; however, the system time is synchronized using the Network Time Protocol ("NTP").

5.5.6. Archive Collection System (Internal or External)

Apple Pubic CA collects archive information internally.

5.5.7. Procedures to Obtain and Verify Archive Information

Apple restricts all access to archive data to only authorized trusted personnel and Apple staff 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 Sub-CA's lifetime, a new CA Key Pair is generated following the procedures in Section 6.1.1.1. 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 Sub-CA Certificate available to verify signatures until all of the Subscriber Certificates signed with the Private Key have expired.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

As part of Apple Inc., Apple Public CA leverages the organization-wide Disaster Recovery Plan. This plan accounts for responses to a variety of human or nature-driven caused events. The plan relies on a business-risk-based tier classification for systems. Appropriate resources are assigned, and actions planned, depending on the application's tier. Apple Public CA systems are classified in the top tiers.

In addition, Apple Public CA supplements the Disaster Recovery Plan in areas that are unique to a public PKI. Examples include response to compromise of Private Keys used in Sub-CAs and OCSP Responders, notifications to PKI Participants, and awareness and education of Apple Public CA staff.

Apple Public CA's plan includes incident management and reporting. Apple Public CA will address incident reports as outlined in Section 2.4 of the Mozilla Root Store Policy, and the Microsoft Trusted Root Program's Security Incident Response Requirements.

Apple Public CA does not publicly disclose its Disaster Recovery Plan but makes it available to auditors during the annual audit, if requested. Apple Public CA continuously reviews and updates this plan. Disaster recoverability is tested at least once a year.

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. 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 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.

If the investigation confirms the need for revocation, Apple Public CA will request revocation of the compromised Sub-CA Certificate by the Root CA. Subsequently, a new CA Key Pair will be created, and a request to generate a new Sub-CA will be submitted to the Root CA. Apple Public CA will also revoke all impacted Subscriber Certificates.

In some cases, Apple Public CA already has other Sub-CA Certificates in an inactive state. If the compromise event did not affect those assets, those Certificates may be used for issuance of Subscriber Certificates.

5.7.4. Business Continuity Capabilities After a Disaster

The Disaster Recovery Plan discussed 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, Apple Public CA will execute the termination plan that addresses the following:

- Provision of notice to related parties affected by the termination,
- The revocation of Certificates issued by the CA,
- The preservation of the 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

Apple Public CA generates CA Key Pairs used in Sub-CA Certificates during a scripted ceremony, conducted by trusted personnel observing separation of duties consistent with Section 5.2, witnessed by external qualified auditors, and/or video recorded. 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

Apple Public CA does not generate Key Pairs for TLS Server Certificates, signing-only S/MIME Certificates, or S/MIME Certificates used for encryption for which the Subscriber did not provide escrow authorization. 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. When Apple Public CA generates Key Pairs used in certain S/MIME Certificates the generated keys meet size requirements in Section 6.1.5 and parameters in Section 6.1.6.

Apple Public CA does not allow key re-use, which prevents known compromised keys associated with revoked Certificates or rejected Certificate Applications to be used in a new Certificate Application.

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 used for encryption purposes and for which escrow is authorized by the Subscriber, 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

Except for Certificates specified below, Public Keys are submitted using a PKCS#10 CSR over a TLS connection.

For S/MIME Certificates that include the Commit Signing purpose in the Extended Key Usage, the Public Key is extracted from the Certificate-based Identification Credential used to authenticate to the enrollment system with a mutually authenticated TLS session (see Section 3.2.1)

6.1.4. CA Public Key Delivery to Relying Parties

Apple Public CA does not issue Root CA Certificates, as such, it relies on its providers and Application Software Providers to distribute those Certificates.

Sub-CA Certificates are hosted online and can be reached through a URL provided in the 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 CA Certificates

No stipulation.

6.1.5.2. Sub-CA Certificates

Apple Public CA does not issue Sub-CA Certificates. Instead, it works with its Root CA providers to meet the requirements specified in the Baseline Requirements Section 6.1.5.

Apple Public CA generates CA Key Pairs for its 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

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 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 may also confirm the modulus is an odd number, not the power of a prime and has no factors smaller than 752.

For ECDSA keys, the enrollment 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 use of a specific key is determined by the Key Usage and Extended Key Usage extensions in the X.509 Certificate. Apple Public CA uses in its TLS and S/MIME Certificates only the Key Usage and Extended Key Usage extension values defined in Section 7.1.2.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

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

For Organization-validated Multipurpose SMIME Certificates with the Commit Signing purpose, Private Keys are generated and stored in Cryptographic Modules that are selected based on features that: 1) prevent the export of Private Key, and 2) have key residency proof mechanisms.

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

Sub-CA Private Keys, including backups, are protected with multi-person control which requires a minimum of two individuals in Trusted Roles.

6.2.3. Private Key Escrow

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

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

6.2.4. Private Key Backup

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

6.2.5. Private Key Archival

Apple Public CA does not archive its CA Private Keys.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

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

6.2.7. Private Key Storage on Cryptographic Module

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

Private Keys used in Organization-validated Multipurpose SMIME Certificates with the Commit Signing purpose are generated in selected hardware Cryptographic Modules described in Section 6.2.1. .

6.2.8. Method of Activating Private Key

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

For Organization-validated Multipurpose SMIME Certificates on hardware, activation data consists of two-factor authentication (i.e., something you have, something you are, or something you know). For the something-you-know factor, the number of failed attempts is limited and when exceeded, the Cryptographic Module is locked and the key can no longer be used.

6.2.9. Method of Deactivating Private Key

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

6.2.10. Method of Destroying Private Key

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

The Public Key is archived as part of the Certificate archival.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Certificate Validity and Key Operational periods are shown below.

Certificate Type	Key Operational Period	Certificate Validity
Sub-CA	Up to 15 years	Up to 15 years
TLS	Up to 396 days	Up to 396 days
S/MIME	Up to 824 days	Up to 824 days
OCSP Responder	Up to 90 days	Up to 90 days

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

Apple Public CA follows the manufacturer specifications for the activation data required for 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

Apple Public CA protects data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Secure tokens with activation data are kept under 2-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 to systems or applications are permitted,
- User privileges are managed to limit users to their assigned roles,
- Audit records are generated and archived for applicable transactions,
- Enforce domain integrity boundaries 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

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

Apple 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, 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

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 Apple Public CA generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG for use in end-entity Certificates.

7.1.1. Version Numbers

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

7.1.2. Certificate Content and Extensions

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

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

Apple Public CA does not issue Root CA Certificates.

7.1.2.2. Cross-Certified Subordinate CA Certificate Profile

Apple Public CA does not issue Cross-Certified Sub-CA Certificates. Apple Public CA works together with Root CA provider(s) to obtain compliant Cross-Certified Sub-CA Certificates as needed.

7.1.2.3. Technically Constrained Non-TLS Subordinate CA Certificate Profile

Apple Public CA does not issue Technically Constrained Non-TLS Sub-CA Certificates. Apple Public CA works together with Root CA provider(s) to obtain compliant technically-constrained non-TLS Sub-CA Certificates as needed.

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

Apple Public CA does not issue Technically Constrained Non-TLS Sub-CA Certificates. Apple Public CA works together with Root CA provider(s) to obtain compliant technically-constrained TLS Sub-CA Certificates as needed.

7.1.2.6. Unconstrained Subordinate CA Certificate Profile

Apple Public CA does not issue unconstrained Sub-CA Certificates. Apple Public CA works together with Root CA provider(s) to obtain compliant unconstrained Sub-CA Certificates as needed.

The Apple Public CA has been issued unconstrained S/MIME Sub-CAs that meet the definition of Extant S/MIME CAs. Those Extant S/MIME CAs will 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. New compliant Sub-CAs will be in place by September 15, 2024.

7.1.2.7. Subscriber Certificate Profile

The Apple Public CA issues TLS Server Certificates of types Organization Validated (OV), Extended Validation (EV), and S/MIME Certificates of types Mailbox-validated Strict, Organization-validated Strict and Multipurpose. The following tables summarize the profiles for all 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.

Field	Description
subject	Subject content varies depending on certificate type (OV, EV). Encoding, length and order is specified in Section 7.1.4.2 EV TLS - Business Category, - Jurisdiction Country, - Jurisdiction State, - Serial Number, - Country, - State, - Locality, - Organization, - Common Name. OV TLS - Country, - State, - 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	-

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
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)

Extension	Presence	Critical	Content
certificatePolicies (Note 2)	Yes	No	EV TLS - Policy OID 1: 2.23.140.1.1 - Policy OID 2: 2.16.840.1.114412.2.1 OV TLS - Policy OID 1: 2.23.140.1.2.2 - Policy OID 2: 1.2.840.113635.100.5.11.4 Both Certificate types also include this qualifier: - 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, clientAuth (Note 3)
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: (Note 4) 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	At least one extension that complies with Section 7.1.2.11.5

Note 1: The dnsName field contains either 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 dnsName field 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/"

Note 3: The Client Authentication purpose may be omitted.

Note 4: The Key Agreement purpose is being removed from TLS Server Certificates starting on August 31, 2022. Some legacy Certificates may exhibit this purpose by the time of publication of this CPS version.

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 / Multipurpose or Pre-S/MIME Baseline Requirements Legacy). Encoding, length and order is specified in Section 7.1.4.2 Mailbox-validated Strict - Email Organization-validated Strict / Multipurpose - Country, - State, - Organization, - Organization Identifier, - Common Name. Pre-S/MIME Baseline Requirements Legacy Certificate - Common Name, - Organization, - Organization Identifier, - State, - Country.
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
subjectAltName	Yes	No	rfc822Name (minimum of 1, maximum of 1) (Note 1)

Extension	Presence	Critical	Content
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 Organization-validated Multipurpose - Policy OID: 2.23.140.1.5.2.2 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" Commit Signing: Apple Trust Attribute Apple (Note 5) - Policy OID: 1.2.840.113635.100.5.21.1 Commit Signing: Apple Trust Attribute Hardware (Note 5) - Policy OID: 1.2.840.113635.100.5.21.2 Commit Signing: Apple Trust Attribute Multi Factor Authentication (Note 5) - Policy OID: 1.2.840.113635.100.5.21.3 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 Organization-validated Multipurpose: emailProtection, clientAuth (Note 3), Apple Commit Signing (Note 4)

Extension	Presence	Critical	Content
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.

Note 3: The Client Authentication purpose may be omitted.

Note 4: Commit Signing purpose to be included in SMIME Organization-validated Multipurpose Certificates, which is identified with an OID residing within an Apple-owned arc. OID: 1.2.840.113635.100.4.20.

Note 5: Certificates with the Commit Signing purpose have their keys generated/stored on hardware. Hardware generation/storage is indicated with one or two policy OIDs. Commit Signing: Apple Trust Attribute Hardware policy OID is always present. Commit Signing: Multi Factor Authentication is present when hardware activation data is required to use the Private Key. The Commit Signing: Apple Trust Attribute Apple is present when Apple-manufactured hardware is used.

7.1.2.8. OCSP Responder Certificate Profile

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

Field	Description
validity	notAfter: notBefore is the time of signing. notAfter: a value not to exceed what is specified in Section 6.3.2.
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	Yes	Yes	cA = False pathLenConstraint is not present
authorityKeyIdentifier	Yes	No	keyIdentifier complies with Section 7.1.2.11.1
authorityInfoAccess	No	-	-
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
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

While Apple Pubic CA does not issue Sub-CA Certificates, it collaborates with Root CA provider(s) to issue Certificates with validities that do not exceed the values in Section 6.3.2.

7.1.2.10.2. CA Certificate Naming

While Apple Pubic CA does not issue Sub-CA Certificates, it collaborates with Root CA provider(s) to issue Certificates that contain Subject DNs that meet naming structure below.

Attribute	Presence	Value
countryName	Yes	US
stateOrProvinceName	Yes	California
organizationName	Yes	Apple Inc.
commonName	Yes	Legacy Common Name: Apple IST CA [number] – G1 Current Common Name: Apple Public [type] [technology] CA [number] – G[generation] Where: Type: A string identifying the type of Certificates issued under the CA. For example: "EV Server", "Server" or "Client" Technology: A string representing the technology used for issued Certificates. For example, "ECC" or "RSA". Number: A numeric value that uniquely distinguishes the issuing CA root from others. Generation: A numeric value that starts with one (1) and increases by one (1) when a new Certificate is issued under a particular "number".

7.1.2.11. Common Certificate Fields

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 all Subscriber Certificates and is not present in 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	-
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

This section discusses all extensions and extension values not addressed by the applicable certificate profile in S/MIME Baseline Requirements Section 71.2.7. Extensions included here:

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

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)	300d06092a864886f70d0101 010500
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: 301306072a8648ce3d02010 6082a8648ce3d030107 secp384r1: 301006072a8648ce3d02010 6052b81040022

7.1.3.2. Signature AlgorithmIdentifier

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	300d06092a864886f70d0101 0b0500
sha384WithRSAEncryption 1.2.840.113549.1.1.12	RSASSA-PKCS1-v1_5 with SHA-384	300d06092a864886f70d0101 0c0500
For P-256 signing key only: ecdsa-with-SHA256 1.2.840.10045.4.3.2	ECDSA with SHA-256	300a06082a8648ce3d04030 2

Algorithm (Object Identifier)	Parameter	Hexadecimal Parameter Encoding
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 Subscriber Certificates, the encoded content of the Issuer Distinguished Name matches byte-for-byte the encoded form of the Subject Distinguished Name field of the Issuing CA Certificate.

Apple Public CA encodes Subscriber 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 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.

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	
			OV TLS	EV TLS
businessCategory	UTF8String or PrintableString	128	-	Yes
jurisdictionCountry	PrintableString	2	-	Yes
jurisdictionStateOrProvince	UTF8String or PrintableString	128	-	Yes
serialNumber	PrintableString	64	-	Yes
countryName	PrintableString	2	Yes	Yes
stateOrProvinceName	UTF8String or PrintableString	128	Yes	Yes
localityName	UTF8String or PrintableString	128	-	Yes
organizationName	UTF8String or PrintableString	64	Yes	Yes
commonName	UTF8String or PrintableString	64	Yes	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.

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

Attribute	Encoding	Max Length	Presence (Note 1)		
			MVS	OVM	OVS
commonName (Note 3)	UTF8String or PrintableString	64	No	Yes	Yes

Note 1: Mailbox-Validated-Strict (MVS), Organization-Validated-Multipurpose (OVM), OrganizationValidated-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.

The table below applies to S/MIME Certificates issued prior to September 1, 2023, which do not comply with the SMIME Baseline Requirements version 1.0.1. Such Certificates will be allowed to expire.

Attribute	Encoding	Max Length	Presence
commonName	UTF8String	64	Yes
organizationName	PrintableString	64	Yes
serialNumber	PrintableString	64	Optional (Note 1)
stateOrProvinceName	PrintableString	128	Yes
countryName	PrintableString	2	Yes
organizationIdentifier	UTF8String	None	Optional (Note 2)

Note 1: The serialNumber attribute was not used in all implementations. This field contains the Registration Number assigned to a Private Organization by the Incorporating Agency in such entity's Jurisdiction of Incorporation.

Note 2: The organizationIdentifier attribute was not used in all implementations.

OCSP Responder Certificates

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

Attribute	Encoding	Max Length	Presence
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 Addresses contained in the Subject DN's commonName or emailAddress field, 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.

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	EV	S/MIME	
dNSName	Required	Required		A verified Wildcard Domain Name or FQDN Internal Names are not allowed For EV Certificates: Wildcard Domain 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 Email 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 Apple Public CA contain the CertificatePolicy extension populated with at least one policy OID.

Policy OIDs included in Apple Public CA issued Certificates are specified in Section 7.1.6.1.

7.1.6.1. Reserved Certificate Policy Identifiers

The following policy OIDs are reserved by the CA/Browser Forum and the Apple Public CA, or its vendors, for use by Apple Public CA as a means of asserting that a Certificate complies with the Baseline Requirements, the EV Guidelines and S/MIME Baseline Requirements. 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)

Extended Validation

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines(1)} (2.23.140.1.1)

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

Organization Validated

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleCABFSSLBaselineCertificatePolicy(4)} (1.2.840.113635.100.5.11.4)

Extended Validation

{joint-iso-ccitt(2) country(16) USA (840) US-company(1) DigiCert(114412)} (2.16.840.1.114412) ev-ssl-certificates (2)(1) (2.16.840.1.114412.2.1)

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),

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleISTEmailCertificatePolicyIDs (5) MailboxLegacy (4)} (1.2.840.113635.100.5.11.5.4),

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleISTEmailCertificatePolicyIDs (5) OrganizationLegacy (5)} (1.2.840.113635.100.5.11.5.5),

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleISTEmailCertificatePolicyIDs (5) SponsorLegacy (6)} (1.2.840.113635.100.5.11.5.6), 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.*6–15*); where n may be a number between 7 and 15, inclusive.

Hardware Cryptographic Module Generation/Storage

The following policy OIDs are used to indicate the use of a hardware Cryptographic Module for generation and storage of a key pair associated with Organization-validated Multipurpose SMIME Certificates that include the Commit Signing purpose. These policy OIDs are always paired with a CABF policy OID.

The appleTrustAttributePublicCommitSigningHardware policy OID is always present. The appleTrustAttributePublicCommitSigningApple is present when Apple-manufactured hardware is used.

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) appleTrustAttributesPublicCommitSigning (21) appleTrustAttributePublicCommitSigningApple (1)} (1.2.840.113635.100.5.21.1)

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) appleTrustAttributesPublicCommitSigning (21) appleTrustAttributePublicCommitSigningHardware (2)} (1.2.840.113635.100.5.21.2)

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) appleTrustAttributesPublicCommitSigning (21) appleTrustAttributePublicCommitSigningMultifactor (3)} (1.2.840.113635.100.5.21.3)

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) appleTrustAttributesPublicCommitSigning (21) m} (1.2.840.113635.100.5.21.4–5); where m may be 4 or 5, inclusive.

7.1.6.1.3. Reserved Policy OIDs Equivalence

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

Certificate Type	CABF Forum Reserved	Apple or Vendor Reserved
TLS - Organization Validated	2.23.140.1.2.2	1.2.840.113635.100.5.11.4
TLS - Extended Validation	2.23.140.1.1	2.16.840.1.114412
S/MIME - Mailbox-validated Strict	2.23.140.1.5.1.3	-
S/MIME - Organization-validated Multipurpose	2.23.140.1.5.2.2	-
S/MIME - Organization-validated Strict	2.23.140.1.5.2.3	-

Certificate Type	CABF Forum Reserved	Apple or Vendor Reserved
S/MIME - Pre-SBR Sponsor SignEncrypt	-	1.2.840.113635.100.5.11.5.1
S/MIME - Pre-SBR Sponsor Sign	-	1.2.840.113635.100.5.11.5.2
S/MIME - Pre-SBR Sponsor Encrypt	-	1.2.840.113635.100.5.11.5.3
S/MIME - Pre-SBR MailboxLegacy	-	1.2.840.113635.100.5.11.5.4
S/MIME - Pre-SBR OrganizationLegacy	-	1.2.840.113635.100.5.11.5.5
S/MIME - Pre-SBR SponsorLegacy	-	1.2.840.113635.100.5.11.5.6
S/MIME - Pre-SBR FutureUse	-	1.2.840.113635.100.5.11.5.7 — 1.2.840.113635.100.5.11.5.15
S/MIME - Organization-validated Multipurpose, Commit Signing purpose, and Apple Hardware	-	1.2.840.113635.100.5.21.1
S/MIME - Organization-validated Multipurpose, Commit Signing purpose, and non-Apple Hardware	-	1.2.840.113635.100.5.21.2
S/MIME - Organization-validated Multipurpose, Commit Signing purpose, and Multi Factor Authentication	-	1.2.840.113635.100.5.21.3
S/MIME - Organization-validated Multipurpose, Commit Signing purpose, and hardware generation - future use	-	1.2.840.113635.100.5.21.4 — 1.2.840.113635.100.5.21.5

7.1.6.2. Root CA Certificates

Apple Public CA does not issue Root CA Certificates.

7.1.6.3. Subordinate CA Certificates

Apple Public CA does not issue Cross-Certified Sub-CA Certificates.

7.1.6.4. Subscriber Certificates

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

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 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 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)
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 (See Note 1), it is not marked critical when present: • superseded • cessationOfOperation • affiliationChanged (See Note 2) • keyCompromise • privilegeWithdrawn (See Note 2) 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 affiliationChanged and privilegeWithdrawn reason codes are not made available for selection by the Subscriber as only the Apple Public CA can conclusively verify causes 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	Yes	Conditional (Note 1)	The distributionPoint field contains a HTTP URL to CRL

Note 1: Issuing Distribution Point is Required when a CRL does not contain all the entries for revoked unexpired certificates issued by the CRL issuer ("Partitioned" CRL).

7.3. OCSP PROFILE

7.3.1. Version Number

OCSP responses conform to RFC 6960, Version 1. OCSP responses will include the following fields:

- Signature Algorithm: a signature algorithm specified in Section 7.1.3.2.
- Responder's Identifier: the OCSP responder's Public Key SHA1 hash
- Produced At: the 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
- This Update: the time at which the status indicated is known to the responder to be correct
- Next Update: the time at which newer information will be available

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 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 TLS Server Certificates, the auditor will also assess controls to the then-current standards:

- CPA Canada Trust Service Principles and Criteria for Certification Authorities
- CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
- CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation for SSL (for EV Certificates only)

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

- CPA Canada WebTrust 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.

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

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Apple Public CA will retain the external audit firm, and individual auditors shall not be employees or related to employees of Apple.

8.4. TOPICS COVERED BY ASSESSMENT

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

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

Apple Public CA works with its auditor to ensure audit reports conform with the content and format requirements in the CAB Forum Baseline Requirements Section 8.6, Mozilla Root Store Policy Section 3.1.4 and the Common CA Database Section 5.1. Audit results are communicated to the Apple CA Policy Authority and to others as deemed appropriate based on agreements, regulations, and law. Apple Public CA submits audit results to its Root CA providers.

Copies of the latest audit reports can be found in Apple Public CA's Repository as specified in Section 2.1. 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, Apple Public CA performs regular internal audits against at least three percent (3%) of Certificates issued since the last internal audit.

Apple Public CA automatically validates all 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.

Additionally, Apple Public CA performs quarterly internal audits against issued EV Certificates to confirm they were approved according to the validation practices defined in Section 3 and Section 4.

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

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

9.1.2. Certificate Access Fees

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

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. 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

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. 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 Public CA maintains Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

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 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,
- CA public Certificates,
- Information contained in this CPS document, 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

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. .

Root CA Private Keys, Public Keys and Certificates remain the property of the Root CA providers listed in Appendix A.

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).

For EV Certificates, Apple represents to Subscribers, Subjects, Application Software Vendors that distribute Apple Public CA Certificates, and Relying Parties that use an Apple Public CA Certificates while the Certificate is valid that Apple followed the EV Guidelines when verifying information and issuing EV Certificates.

This representation is limited solely to Apple Public CA's compliance with the EV Guidelines (e.g., Apple may rely on erroneous information provided in an attorney's opinion or accountant's letter or Subscriber representations that is checked in accordance with the Guidelines).

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 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 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 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 Apple Public CA it:

- Obtained sufficient knowledge on the use of digital 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, and
- any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.
- 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 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 Apple Public CA.

To the extent 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'. 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 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 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 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 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 Policy Authority.

9.12.2.Notification Mechanism and Period

Apple Public CA posts CPS revisions to its Repository, see Section 2.1. 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 Apple Public CA and attempt to resolve disputes directly with 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. 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 Subordinate CAs Hierarchy

This table lists all valid Sub-CA Certificates issued to Apple Public CA by publicly-trusted Root CA providers. The list is organized alphabetically using the Root CA Certificate Common Name first and then Sub-CA Certificate Common Name. The Root CA Provider CP lists the name of the Root CA provider, which is correlated with the following Certificate Policies:

- DigiCert: https://www.digicert.com/legal-repository/
- Sectigo: https://sectigo.com/legal

Root CA Common Name	Root CA Provider CP	Sub-CA Common Name	Sub-CA Serial Number	Subscriber Certificates
AAA Certificate Services	Sectigo	Apple Public Client RSA CA 12 - G1	00:CB:79:51:3F:DF:5A:41:B7:EB:A3:B5:01:2C:66:57:62	S/MIME Certificates
		Apple Public Server RSA CA 12 - G1	0A:E4:8F:23:01:30:64:41:92:59:E1:C2:9A:E9:8D:18	TLS Server Certificates
		Apple Public Server ECC CA 12 - G1	72:66:18:75:3A:D6:C9:22:C5:6C:9D:E1:F3:84:78:B0	TLS Server Certificates
Baltimore CyberTrust Root	DigiCert	Apple IST CA 2 – G1	05:52:C7:EF:FE:EC:29:2B:A9:F1:38:7B:07:AF:92:9F	TLS Server Certificates
		Apple IST CA 8 – G1	0A:48:D5:7C:65:FB:0E:6C:F7:04:A3:64:5F:14:18:E4	TLS Server Certificates
		Apple Public Server ECC CA 2 – G1	05:AE:CA:D3:A2:D2:46:D5:87:EC:93:91:71:1D:11:14	TLS Server Certificates
		Apple Public Server RSA CA 2 – G1	0B:79:9A:EF:7B:9D:ED:2B:41:8B:8D:3E:AA:3A:8F:7C	TLS Server Certificates
COMODO ECC Certification Authority	Sectigo	Apple Public Server ECC CA 11 - G1	00:98:C1:72:76:AA:83:69:08:DC:DC:5B:4E:F8:BD:41:74	TLS Server Certificates
DigiCert Global Root G2	DigiCert	Apple Public EV Server RSA CA 1 – G1	04:F2:2E:CC:21:FC:B4:38:2A:C2:8B:8F:2D:64:1F:C0	EV Certificates
		Apple Public Server RSA CA 1 – G1	0F:D2:A1:06:FC:12:F6:06:DB:E5:12:7F:BE:16:68:12	TLS Server Certificates
DigiCert Global Root G3	DigiCert	Apple IST CA 8 – G1 (without OU)	05:AE:84:C4:40:6C:98:F0:1B:DD:0F:0E:60:20:FE:9A	TLS Server Certificates
		Apple IST CA 8 – G1	0C:67:62:07:77:A5:AB:C4:BA:53:5D:8D:AD:CF:9A:D7	TLS Server Certificates

Root CA Common Name	Root CA Provider CP	Sub-CA Common Name	Sub-CA Serial Number	Subscriber Certificates
		Apple Public EV Server ECC CA 1 – G1	0C:AB:AA:D1:CE:C4:E9:7C:C2:66:58:81:D0:21:38:F7	EV Certificates
		Apple Public Server ECC CA 1 – G1	06:B4:54:3F:F3:3B:B1:98:27:C1:87:A0:21:3E:C1:1A	TLS Server Certificates
DigiCert High Assurance EV Root CA	DigiCert	Apple Public EV Server RSA CA 2 – G1	07:17:79:11:00:5D:22:67:F6:88:92:F6:8F:8B:50:58	EV Certificates
		Apple Public EV Server RSA CA 3 – G1	06:9A:C4:39:BB:31:C1:1A:B2:91:40:25:C:AE:15:D7	EV Certificates
GeoTrust Global CA	DigiCert	Apple IST CA 2 – G1	00:02:3A:74	TLS Server Certificates (Legacy)
GeoTrust Primary CA G2	DigiCert	Apple IST CA 8 – G1	13:52:2E:BF:C1:DD:5C:E1:1E:F2:76:40:75:1F:E7:DF	TLS Server Certificates (Legacy)
USERTrust RSA Certification Authority	Sectigo	Apple Public Client RSA CA 11 - G1	4E:41:83:94:B2:40:A7:CC:A8:E7:6A:AE:9D:84:97:93	S/MIME Certificates
		Apple Public Client RSA CA 13 - G1	01:10:B4:ED:58:16:D0:8C:A5:07:96:30:5D:1E:85:52	S/MIME Certificates
		Apple Public Server RSA CA 11 - G1	5D:FA:BB:95:77:CF:AB:67:1F:C7:DD:FE:D1:CF:20:5B	TLS Server Certificates
		Apple Public Client RSA CA 50 - G1	75:7F:BA:FF:E6:4A:1D:80:BA:C7:83:DF:A8:CA:E2:13	S/MIME Certificates
USERTrust ECC Certification Authority	Sectigo	Apple Public Client ECC CA 11 - G1	77:EA:E0:D5:09:78:C4:21:CC:2E:1B:29:F1:31:9D:54	S/MIME Certificates
		Apple Public Client ECC CA 50 - G1	00:B6:BA:1D:80:2E:9C:27:40:FC:A4:06:53:FA:66:FA:57	S/MIME 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
September 24, 2020	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 some 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 CA/Browser 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.
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.