

**Apple Inc.**  
Certification Practice Statement  
Apple Public CA

Version 5.0  
Effective Date: April 29, 2020



# Table of Contents

<b>1. INTRODUCTION</b> .....	<b>1</b>
<b>1.1. OVERVIEW</b> .....	<b>1</b>
<b>1.2. DOCUMENT NAME AND IDENTIFICATION</b> .....	<b>2</b>
1.2.1. Revisions.....	4
<b>1.3. PKI PARTICIPANTS</b> .....	<b>6</b>
1.3.1. Certification Authorities .....	6
1.3.2. Registration Authorities .....	6
1.3.3. Subscribers .....	6
1.3.4. Relying Parties .....	7
1.3.5. Other Participants.....	7
<b>1.4. CERTIFICATE USAGE</b> .....	<b>7</b>
1.4.1. Appropriate Certificate Uses .....	7
1.4.2. Prohibited Certificate Uses.....	7
<b>1.5. POLICY ADMINISTRATION</b> .....	<b>8</b>
1.5.1. Organization Administering the Document.....	8
1.5.2. Contact Person.....	8
1.5.3. Person Determining CPS Suitability for the Policy.....	8
1.5.4. CPS Approval Procedures .....	8
<b>1.6. DEFINITIONS AND ACRONYMS</b> .....	<b>8</b>
1.6.1. Definitions.....	8
1.6.2. Acronyms .....	10
1.6.3. References.....	10
1.6.4. Conventions.....	11
<b>2. PUBLICATION AND REPOSITORY RESPONSIBILITIES</b> .....	<b>12</b>
<b>2.1. REPOSITORIES</b> .....	<b>12</b>
<b>2.2. PUBLICATION OF CERTIFICATION INFORMATION</b> .....	<b>12</b>
<b>2.3. TIME OR FREQUENCY OF PUBLICATION</b> .....	<b>12</b>
<b>2.4. ACCESS CONTROLS ON REPOSITORIES</b> .....	<b>13</b>
<b>3. IDENTIFICATION AND AUTHENTICATION</b> .....	<b>14</b>
<b>3.1. NAMING</b> .....	<b>14</b>
3.1.1. Types of Names .....	14
3.1.2. Need for Names to be Meaningful.....	14
3.1.3. Anonymity or Pseudonymity of Subscribers .....	14



3.1.4.	Rules of Interpreting Various Name Forms .....	14
3.1.5.	Uniqueness of Names .....	14
3.1.6.	Recognition, Authentication, and Role of Trademarks .....	15
<b>3.2.</b>	<b>INITIAL IDENTITY VALIDATION.....</b>	<b>15</b>
3.2.1.	Method to Prove Possession of Private Key .....	15
3.2.2.	Authentication of Organization Identity,Domain Identity and Email Control.....	15
3.2.3.	Authentication of Individual Identity.....	18
3.2.4.	Non-Verified Subscriber Information.....	18
3.2.5.	Validation of Authority .....	19
3.2.6.	Criteria for Interoperation .....	20
<b>3.3.</b>	<b>IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS .....</b>	<b>20</b>
3.3.1.	Identification and Authentication for Routine Re-Key.....	20
3.3.2.	Identification and Authentication for Re-Key After Revocation .....	20
<b>3.4.</b>	<b>IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS .....</b>	<b>20</b>
<b>4.</b>	<b>CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS .....</b>	<b>21</b>
<b>4.1.</b>	<b>CERTIFICATE APPLICATION .....</b>	<b>21</b>
4.1.1.	Who Can Submit a Certificate Application .....	21
4.1.2.	Enrollment Process and Responsibilities .....	21
<b>4.2.</b>	<b>CERTIFICATE APPLICATION PROCESSING .....</b>	<b>22</b>
4.2.1.	Performing Identification and Authentication Functions .....	22
4.2.2.	Approval or Rejection of Certificate Applications .....	23
4.2.3.	Time to Process Certificate Applications.....	23
<b>4.3.</b>	<b>CERTIFICATE ISSUANCE.....</b>	<b>24</b>
4.3.1.	CA Actions During Certificate Issuance.....	24
4.3.2.	Notification To Subscriber by the CA of Issuance of Certificate.....	24
<b>4.4.</b>	<b>CERTIFICATE ACCEPTANCE .....</b>	<b>24</b>
4.4.1.	Conduct Constituting Certificate Acceptance.....	24
4.4.2.	Publication of the Certificate by the CA .....	24
4.4.3.	Notification of Certificate Issuance by the CA to Other Entities .....	24
<b>4.5.</b>	<b>KEY PAIR AND CERTIFICATE USAGE.....</b>	<b>24</b>
4.5.1.	Subscriber Private Key and Certificate Usage .....	24
4.5.2.	Relying Party Public Key and Certificate Usage .....	25
<b>4.6.</b>	<b>CERTIFICATE RENEWAL .....</b>	<b>25</b>
4.6.1.	Circumstance for Certificate Renewal.....	25



4.6.2. Who May Request Renewal .....	25
4.6.3. Processing Certificate Renewal Requests .....	25
4.6.4. Notification of New Certificate Issuance to Subscriber .....	25
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate .....	25
4.6.6. Publication of the Renewal Certificate by the CA .....	25
4.6.7. Notification of Certificate Issuance by the CA to Other Entities .....	25
<b>4.7. CERTIFICATE RE-KEY .....</b>	<b>25</b>
4.7.1. Circumstance for Certificate Re-Key .....	26
4.7.2. Who May Request Certification of a New Public Key .....	26
4.7.3. Processing Certificate Re-Keying Requests .....	26
4.7.4. Notification of New Certificate Issuance to Subscriber .....	26
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate .....	26
4.7.6. Publication of the Re-Keyed Certificate by the CA .....	26
4.7.7. Notification of Certificate Issuance by the CA to Other Entities .....	26
<b>4.8. CERTIFICATE MODIFICATION .....</b>	<b>26</b>
4.8.1. Circumstance for Certificate Modification .....	26
4.8.2. Who May Request Certificate Modification .....	26
4.8.3. Processing Certificate Modification Requests .....	26
4.8.4. Notification of New Certificate Issuance to Subscriber .....	26
4.8.5. Conduct Constituting Acceptance of Modified Certificate .....	27
4.8.6. Publication of the Modified Certificate by the CA .....	27
4.8.7. Notification of Certificate Issuance by the CA to Other Entities .....	27
<b>4.9. CERTIFICATE REVOCATION AND SUSPENSION .....</b>	<b>27</b>
4.9.1. Circumstances for Revocation .....	27
4.9.2. Who Can Request Revocation .....	30
4.9.3. Procedure for Revocation Request .....	30
4.9.4. Revocation Request Grace Period .....	30
4.9.5. Time Within Which CA Must Process the Revocation Request .....	30
4.9.6. Revocation Checking Requirement for Relying Parties .....	31
4.9.7. CRL Issuance Frequency .....	31
4.9.8. Maximum Latency for CRLs .....	31
4.9.9. On-Line Revocation/Status Checking Availability .....	31
4.9.10. On-Line Revocation Checking Requirements .....	31
4.9.11. Other Forms of Revocation Advertisements Available .....	31



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



5.3.6. Sanctions for Unauthorized Actions .....	38
5.3.7. Independent Contractor Requirements .....	38
5.3.8. Documentation Supplied to Personnel .....	38
<b>5.4. AUDIT LOGGING PROCEDURES.....</b>	<b>38</b>
5.4.1. Types of Events Recorded .....	38
5.4.2. Frequency of Processing Log .....	39
5.4.3. Retention Period for Audit Log .....	39
5.4.4. Protection of Audit Log.....	39
5.4.5. Audit Log Backup Procedures .....	40
5.4.6. Audit Collection System (Internal Vs. External) .....	40
5.4.7. Notification To Event-Causing Subject.....	40
5.4.8. Vulnerability Assessments .....	40
<b>5.5. RECORDS ARCHIVAL.....</b>	<b>40</b>
5.5.1. Types of Records Archived .....	40
5.5.2. Retention Period for Archive .....	41
5.5.3. Protection of Archive.....	41
5.5.4. Archive Backup Procedures .....	41
5.5.5. Requirements for Time-Stamping of Records.....	42
5.5.6. Archive Collection System (Internal or External) .....	42
5.5.7. Procedures to Obtain and Verify Archive Information.....	42
<b>5.6. KEY CHANGEOVER.....</b>	<b>42</b>
<b>5.7. COMPROMISE AND DISASTER RECOVERY .....</b>	<b>42</b>
5.7.1. Incident and Compromise Handling Procedures.....	42
5.7.2. Computing Resources, Software, and/or Data Are Corrupted .....	43
5.7.3. Entity Private Key Compromise Procedures .....	43
5.7.4. Business Continuity Capabilities After a Disaster .....	43
<b>5.8. CA OR RA TERMINATION.....</b>	<b>43</b>
<b>6. TECHNICAL SECURITY CONTROLS .....</b>	<b>45</b>
<b>6.1. KEY PAIR GENERATION AND INSTALLATION.....</b>	<b>45</b>
6.1.1. Key Pair Generation .....	45
6.1.2. Private Key Delivery to Subscriber .....	45
6.1.3. Public Key Delivery to Certificate Issuer.....	45
6.1.4. CA Public Key Delivery to Relying Parties.....	45
6.1.5. Algorithm Type and Key Sizes.....	46



6.1.6.	Public Key Parameters Generation and Quality Checking.....	46
6.1.7.	Key Usage Purposes (as per X.509 v3. Key Usage Field) .....	47
<b>6.2.</b>	<b>PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....</b>	<b>47</b>
6.2.1.	Cryptographic Module Standards and Controls .....	47
6.2.2.	Private Key (n out of m) Multi-Person Control.....	47
6.2.3.	Private Key Escrow .....	47
6.2.4.	Private Key Backup.....	47
6.2.5.	Private Key Archival .....	47
6.2.6.	Private Key Transfer Into or From a Cryptographic Module .....	47
6.2.7.	Private Key Storage on Cryptographic Module.....	47
6.2.8.	Method of Activating Private Key .....	47
6.2.9.	Method of Deactivating Private Key.....	48
6.2.10.	Method of Destroying Private Key .....	48
6.2.11.	Cryptographic Module Rating .....	48
<b>6.3.</b>	<b>OTHER ASPECTS OF KEY PAIR MANAGEMENT.....</b>	<b>48</b>
6.3.1.	Public Key Archival .....	48
6.3.2.	Certificate Operational Periods and Key Pair Usage Periods .....	48
<b>6.4.</b>	<b>ACTIVATION DATA .....</b>	<b>48</b>
6.4.1.	Activation Data Generation and Installation .....	48
6.4.2.	Activation Data Protection.....	49
6.4.3.	Other Aspects of Activation Data.....	49
<b>6.5.</b>	<b>COMPUTER SECURITY CONTROLS.....</b>	<b>49</b>
6.5.1.	Specific Computer Security Technical Requirements .....	49
6.5.2.	Computer Security Rating.....	49
<b>6.6.</b>	<b>LIFE CYCLE TECHNICAL CONTROLS.....</b>	<b>49</b>
6.6.1.	System Development Controls .....	49
6.6.2.	Security Management Controls .....	50
6.6.3.	Life Cycle Security Controls .....	50
<b>6.7.</b>	<b>NETWORK SECURITY CONTROLS.....</b>	<b>50</b>
<b>6.8.</b>	<b>TIME-STAMPING.....</b>	<b>50</b>
<b>7.</b>	<b>CERTIFICATE, CRL, AND OCSP PROFILES .....</b>	<b>51</b>
<b>7.1.</b>	<b>CERTIFICATE PROFILE .....</b>	<b>51</b>
7.1.1.	Version Numbers .....	51



7.1.2.	Certificate Extensions .....	51
7.1.3.	Algorithm Object Identifiers .....	53
7.1.4.	Name Forms .....	53
7.1.5.	Name Constraints .....	55
7.1.6.	Certificate Policy Object Identifier .....	55
7.1.7.	Usage of Policy Constraints Extension .....	55
7.1.8.	Policy Qualifiers Syntax and Semantics .....	55
7.1.9.	Processing Semantics for the Critical Certificate Policies Extension .....	56
<b>7.2.</b>	<b>CRL PROFILE.....</b>	<b>56</b>
7.2.1.	Version Number .....	56
7.2.2.	CRL and CRL Entry Extensions .....	56
<b>7.3.</b>	<b>OCSP PROFILE .....</b>	<b>57</b>
7.3.1.	Version Number.....	57
7.3.2.	OCSP Extensions.....	57
<b>8.</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....</b>	<b>58</b>
8.1.	FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT .....	58
8.2.	IDENTITY/QUALIFICATIONS OF ASSESSOR .....	58
8.3.	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY.....	58
8.4.	TOPICS COVERED BY ASSESSMENT .....	58
8.5.	ACTIONS TAKEN AS A RESULT OF DEFICIENCY.....	58
8.6.	COMMUNICATION OF RESULTS .....	59
8.7.	SELF-AUDITS.....	59
<b>9.</b>	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>60</b>
9.1.	FEES .....	60
9.1.1.	Certificate Issuance or Renewal Fees.....	60
9.1.2.	Certificate Access Fees .....	60
9.1.3.	Revocation or Status Information Access Fees .....	60
9.1.4.	Fees for Other Services .....	60
9.1.5.	Refund Policy.....	60
<b>9.2.</b>	<b>FINANCIAL RESPONSIBILITY.....</b>	<b>60</b>
9.2.1.	Insurance Coverage .....	60
9.2.2.	Other Assets .....	60
9.2.3.	Insurance or Warranty Coverage for End-Entities.....	61
<b>9.3.</b>	<b>CONFIDENTIALITY OF BUSINESS INFORMATION.....</b>	<b>61</b>





9.3.1. Scope of Confidential Information .....	61
9.3.2. Information Not Within the Scope of Confidential Information.....	61
9.3.3. Responsibility To Protect Confidential Information .....	61
<b>9.4. PRIVACY OF PERSONAL INFORMATION.....</b>	<b>61</b>
9.4.1. Privacy Plan.....	61
9.4.2. Information Treated as Private .....	62
9.4.3. Information Not Deemed Private.....	62
9.4.4. Responsibility To Protect Private Information.....	62
9.4.5. Notice and Consent To Use Private Information.....	62
9.4.6. Disclosure Pursuant to Judicial or Administrative Process.....	62
9.4.7. Other Information Disclosure Circumstances.....	62
<b>9.5. INTELLECTUAL PROPERTY RIGHTS .....</b>	<b>62</b>
<b>9.6. REPRESENTATIONS AND WARRANTIES .....</b>	<b>63</b>
9.6.1. CA Representations and Warranties .....	63
9.6.2. RA Representations and Warranties .....	63
9.6.3. Subscriber Representations and Warranties .....	63
9.6.4. Relying Party Representations and Warranties.....	64
9.6.5. Representations and Warranties of Other Participants .....	65
<b>9.7. DISCLAIMERS OF WARRANTIES .....</b>	<b>65</b>
<b>9.8. LIMITATIONS OF LIABILITY .....</b>	<b>65</b>
<b>9.9. INDEMNITIES.....</b>	<b>67</b>
9.9.1. Indemnification by Apple.....	67
9.9.2. Indemnification by Subscribers.....	67
9.9.3. Indemnification By Relying Parties .....	67
<b>9.10. TERM AND TERMINATION .....</b>	<b>68</b>
9.10.1. Term .....	68
9.10.2. Termination.....	68
9.10.3. Effect of Termination and Survival.....	68
<b>9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS .....</b>	<b>68</b>
<b>9.12. AMENDMENTS.....</b>	<b>69</b>
9.12.1. Procedure for Amendment .....	69
9.12.2. Notification Mechanism and Period.....	69
9.12.3. Circumstances Under Which OID Must Be Changed .....	69
<b>9.13. DISPUTE RESOLUTION PROVISIONS.....</b>	<b>69</b>



<b>9.14. GOVERNING LAW .....</b>	<b>69</b>
<b>9.15. COMPLIANCE WITH APPLICABLE LAW .....</b>	<b>69</b>
<b>9.16. MISCELLANEOUS PROVISIONS .....</b>	<b>70</b>
9.16.1. Entire Agreement.....	70
9.16.2. Assignment.....	70
9.16.3. Severability .....	70
9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights) .....	70
9.16.1. Force Majeure.....	70
<b>9.17. OTHER PROVISIONS.....</b>	<b>70</b>
<b>Appendix A: Apple Subordinate CAs Hierarchy .....</b>	<b>71</b>



# 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 exclusively.

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 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”)	<a href="https://cabforum.org/baseline-requirements-documents/">https://cabforum.org/baseline-requirements-documents/</a>
The CAB Forum Guidelines For The Issuance And Management Of Extended Validation Certificates (“EV Guidelines”)	<a href="https://cabforum.org/extended-validation/">https://cabforum.org/extended-validation/</a>
The CAB Forum Network and Certificate System Security Requirements	<a href="https://cabforum.org/network-security-requirements/">https://cabforum.org/network-security-requirements/</a>
Apple Root Store Program	<a href="https://www.apple.com/certificateauthority/ca_program.html">https://www.apple.com/certificateauthority/ca_program.html</a>
Chromium Root Store Policy	<a href="https://www.chromium.org/Home/chromium-security/root-ca-policy">https://www.chromium.org/Home/chromium-security/root-ca-policy</a>
Microsoft Root Certificate Program	<a href="https://docs.microsoft.com/en-us/security/trusted-root/program-requirements">https://docs.microsoft.com/en-us/security/trusted-root/program-requirements</a>



Name of Policy/ Guideline/ Requirement Standard	Location of Source Document
Mozilla Root Store Policy	<a href="https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/">https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/</a>
Oracle Java	<a href="https://www.oracle.com/technetwork/java/javase/javasecarootcertsprogram-1876540.html">https://www.oracle.com/technetwork/java/javase/javasecarootcertsprogram-1876540.html</a>

## 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".

Depending on the type, TLS Certificates regulated by this CPS are issued with at least one Certificate Policy object identifier as shown in the table below. The presence of the policy identifier 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, 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.

For S/MIME Certificates, the presence of the policy identifier asserts that the Apple Public CA makes commercially reasonable efforts to conform to the practices in this CPS for the issuance of those Certificates.

Certificate Type	Policy Object Identifier Label	Policy Object Identifier Numeric Value	Use
TLS: Organization Validated	joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) Certificate-policies(1) baselinerequirements(2) organization-validated(2)	2.23.140.1.2.2	Mandatory



Certificate Type	Policy Object Identifier Label	Policy Object Identifier Numeric Value	Use
	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	Mandatory
TLS: 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	Mandatory
	joint-iso-ccitt(2) country(16) USA (840) US-company(1) DigiCert(114412)	2.16.840.1.114412.2.1	Mandatory
Client: S/MIME only - Sign and Encrypt	iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleSTEmailCertificatePolicyIDs (5) signEncryp (1)	1.2.840.113635.100.5.11.5.1	Mandatory



Certificate Type	Policy Object Identifier Label	Policy Object Identifier Numeric Value	Use
Client: S/MIME only - Sign	iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleSTEmailCertificatePolicyIDs (5) Sign (2)	1.2.840.113635.100.5.11.5.2	Mandatory
Client: S/MIME only - Encrypt	iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleSTEmailCertificatePolicyIDs (5) Encrypt (3)	1.2.840.113635.100.5.11.5.3	Mandatory
Client: Future Use	iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) ist(11) appleSTEmailCertificatePolicyIDs (5)	1.2.840.113635.100.5.11.5.n, where n is 4 – 9.	

### 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 RFC 3647; 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
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.

#### **1.3.3. Subscribers**

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





### **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. 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.

#### **1.3.5.2. 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 a Server Authentication and/or Client Authentication Extended Key Usage 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 Extended Key Usage used to provide secure email. This type of Certificate may also be used to digitally sign an email message from a verified email. For avoidance of doubt, emails associated with a S/MIME Certificate are not intended to replace a written or electronic signature. S/MIME Certificates are only intended to indicate that the email is from an authorized email account, and do not provide any assurance of the identity of the sending party.

### **1.4.2. Prohibited Certificate Uses**

The Apple Public CA does not allow its Certificates to be used to create a Certification Authority nor to allow its Sub-CA Private Keys to sign a Certificate issued by another Certification Authority.

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 contact us at [contact\\_pki@apple.com](mailto:contact_pki@apple.com).
- 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 and 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.
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 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.
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.
Repository	See <a href="#">Section 2.1</a>
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
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DN	Distinguished Name
FQDN	Fully Qualified Domain Name
HSE	High Security Environment
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
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
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 186-4, Federal Information Processing Standards Publication – Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology, July 2013.

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, Chokhani, et al, November 2003.

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

RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006

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

RFC6844, Request for Comments: 6844, DNS Certification Authority Authorization (CAA) Resource Record, Hallam-Baker, Stradling, January 2013.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.

RFC6962, Request for Comments: 6962, Certificate Transparency. B. Laurie, A. Langley, E. Kasper. June 2013.

X.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute Certificate frameworks.

#### **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.



## 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 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.
- This CPS, 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.

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 EV Guidelines, and by Application Software Suppliers. This process is triggered monthly and relies on monitoring the CAB Forum and Application Software Supplier websites for document changes and newly approved ballots.

### 2.2. PUBLICATION OF CERTIFICATION INFORMATION

The latest version of this CPS and agreements are published at [www.apple.com/certificateauthority/public](http://www.apple.com/certificateauthority/public) or [www.apple.com/certificateauthority](http://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](http://www.apple.com/certificateauthority/public) or [www.apple.com/certificateauthority](http://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

Updates to this CPS and updated agreements are published as necessary, but within seven (7) business 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 Distinguished Name ("Subject DN") defined in [Section 7.1.4.2](#); and, a Subject Alternative Name extension defined in [Section 7.1.4.3](#).

##### 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 Certificates include a non-null Subject DN containing the verified information of an entity (i.e. Subscriber), which is either Apple Inc. or one of its subsidiaries. The Fully Qualified Domain Names ("FQDN") included in the Subject Alternative Name extension and Common Name field identify the device(s) controlled by the Subscriber.

S/MIME Certificates include a non-null Subject DN containing the verified information of an entity, which is Apple Inc. or one of its subsidiaries, and the owner of the Domain Name in the verified email address. The Common Name field and the rfc822Name include the email address controlled by the individual requesting the S/MIME Certificate.

##### 3.1.3. Anonymity Or Pseudonymity Of Subscribers

Generally, Apple Public CA does not issue Certificates with pseudonyms; however, for IDNs, Apple Public CA may include the Punycode version of the IDN as a subject name. Apple Public CA may also issue other pseudonymous S/MIME Certificates if they are not prohibited by policy.

##### 3.1.4. Rules of Interpreting Various Name Forms

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

##### 3.1.5. Uniqueness of Names

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

Certificate Type	Uniqueness Determination
TLS Certificate	Inclusion of the domain name in the Certificate. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers ("ICANN").
S/MIME Certificate	Requiring a unique email address.





### **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.

## **3.2. INITIAL IDENTITY VALIDATION**

### **3.2.1. Method To Prove Possession of Private Key**

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

### **3.2.2. Authentication of Organization Identity, Domain Identity and Email Control**

Apple Public CA issues Certificates only to Apple Inc. and its subsidiaries. Subject DN Identity Information for Apple Inc. and its subsidiaries includes the information shown in [Section 7.1.4.2](#), which is validated as explained below.

#### **3.2.2.1. Identity**

For all Certificates, 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.

#### **TLS Certificates and S/MIME Certificates**

Apple Public CA verifies the Applicant’s identity 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,
- A site visit by a representative of the Apple Public CA, or
- An Attestation Letter provided by the Applicant.

#### **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 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.



### **3.2.2.2. DBA/Tradename**

#### **TLS Certificates and 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 to perform the verification.

#### **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 within 20 days of generation of the Random Value.
- (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 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 the .onion Domain Name nor with mixed character sets.

### **3.2.2.5. Authentication for an IP address**

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



### **3.2.2.6. Wildcard domain validation**

Apple Public CA prevents issuance of a Certificate with a wildcard (\*) within the label immediately to the left of a registry-controlled suffix by only approving use of Domain Names not in the publicsuffix.org list, unless they are owned by the Applicant.

### **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 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 Certificate, the Apple Public CA checks 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. 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.

### **3.2.2.10. E-mail Verification**

Prior to issuing an S/MIME Certificate, the Apple Public CA verifies:

- Existence of the Organization in accordance with [Section 3.2.2.1](#),
- The Domain Name contained in the email address is owned or controlled by the entity in the Organization field in accordance with [Section 3.2.2.4](#), and
- Control over the email address by confirming control over the Identification Credential associated with the email, which is used to access the enrollment system to submit the Certificate Application, and the email itself.

### **3.2.2.11. Organization Unit Validation**

For TLS 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 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

#### TLS 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. Certificate Requestors are pre-approved.

#### EV Certificates

Apple Public CA verifies the name, title and agency for Contract Signers and Certificate Approvers; the Contract Signer's Signing Authority and signature in the Terms of Use; and the Certificate Approver's EV Authority using a combination of these EV Guidelines' 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 EV 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 EV 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 EV Authority for future EV 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.

### **3.2.6. Criteria for Interoperation**

No stipulation.

## **3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS**

### **3.3.1. Identification and Authentication for Routine Re-Key**

Not applicable, since Apple Public CA does not provide Certificate re-key as defined in [Section 4.7](#).

### **3.3.2. Identification and Authentication for Re-Key After Revocation**

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

## **3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS**

The Subscriber, or for TLS Certificates, 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 active Apple staff, and its subsidiaries, may submit Certificate Applications.

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, 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.

Apple Public CA uses information produced as a result of suspected phishing or other fraudulent usage or concerns (including revocations and rejected Certificate Applications) to enhance the verification process of Applicant and Domain Name validation in order to identify subsequent suspicious Certificate Applications.

#### 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, email address, and FQDNs,
- Appropriate approvals by authorized Applicant's representatives (for TLS 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 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 Certificates, other than EV: [Section 3.2.2.6](#).

#### S/MIME Certificates

- Email Verification: [Section 3.2.2.10](#),
- Organization: [Section 3.2.2.1](#) and [Section 3.2.2.3](#), 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: 13 months
- Assumed name: 13 months
- Address of Place of Business: 13 months
- Verified Method of Communication: 13 months
- Operational existence: 13 months





- Name, Title, Agency, and Authority: 13 months
- Domain Name for EV: 13 months
- Domain Name for TLS Certificates other than EV and S/MIME: 825 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 from valid Apple staff,
- are not for a Subscriber's owned Domain Name,
- include Domain Names in the list of high risk Domain Names,
- are not for an email address associated to Apple Inc. or its subsidiaries,
- are submitted by Certificate Requestors, or approved by a Certificate Approver, without proper authority.
- 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,
- populate verified data in the Subject DN; and prevent use of fields with metadata such as ":", "-", and " " (i.e., space) characters,
- populate verified FQDNs in the Subject Alternative Names; and prevent use of FQDNs with that include the underscore ("\_") character,
- verify field limitations are respected, for example, the Organization field is 64 characters or shorter.

Apple Public CA may log TLS Certificates to Certificate Transparency logs to ensure the Certificate can operate with Apple and Google clients.

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

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

## **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 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 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, email address) in the Certificate. A renewed Certificate has a new serial number and an expiration date ending after the expiration date of the Certificate being renewed.

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 Renewal Certificate**

No stipulation.

#### **4.6.6. Publication of the Renewal Certificate by the CA**

No stipulation.

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

No stipulation.

### **4.7. CERTIFICATE RE-KEY**

Certificate re-key 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**

#### **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 Certificates**

The Apple Public CA will revoke a TLS 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 TLS Certificate,
2. The Subscriber notifies the Apple Public CA that the original TLS 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 Certificate suffered a Key Compromise, or
4. The Apple Public CA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the TLS Certificate should not be relied upon.

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

1. The TLS 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 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 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 TLS Certificate for a wildcard FQDN 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 Certificate,
7. The Apple Public CA confirms that the TLS Certificate was not issued in accordance with the Baseline Requirements or the CPS,
8. The Apple Public CA confirms that any of the information appearing in the TLS Certificate is inaccurate,
9. The Apple Public CA's right to issue TLS 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, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see <http://wiki.debian.org/SSLkeys>), 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 a S/MIME Certificate after confirming one or more of the following occurred:

1. The Subscriber indicates that the original Certificate Application was not authorized and does not retroactively grant authorization,
2. 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,



3. The Apple Public CA obtains reasonable evidence that the Certificate has been used for a purpose outside of that indicated in the Certificate or in the Terms of Use,
4. 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,
5. The Apple Public CA receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the Certificate is no longer legally permitted,
6. The Apple Public CA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate,
7. A determination that the Certificate was not issued in accordance with the Apple Public CA's CPS,
8. The Apple Public CA determines that any of the information appearing in the Certificate is not accurate,
9. The Apple Public CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate,
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 MozillaRoot 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 Certificates, an authorized Subscriber representative (i.e., Certificate Signer, Certificate Approver, Certificate Requestors) may request the Certificate revocation.

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 indicates that they wish to revoke their Certificate and then the Certificate will be automatically revoked. After the Certificate is revoked a revocation notification is sent to the Subscriber.

After a Certificate Problem Report is received for a TLS Certificate, 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 a 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 every 24 hours. CRLs are issued with a nextUpdate time 7 days from the thisUpdate time. If necessary, emergency CRLs can be generated before the 24-hour period is complete.

#### **4.9.8. Maximum Latency for CRLs**

CRLs are typically posted within 1 hour after generation.

#### **4.9.9. On-Line Revocation/Status Checking Availability**

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

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.

For EV Certificates, CRLs are designed to be downloaded in no more than three (3) seconds over an analog telephone line under normal network conditions.

#### **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.

The status information is updated at least every 4 days and has a maximum expiration time of 10 days.

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 available.



#### **4.9.12.Special Requirements Related to Key Compromise**

In the event of key compromise of the Sub-CA signing key, Apple Public CA will use the practice in [Section 5.7.3](#).

#### **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**

Subscriber Private Keys for S/MIME Certificates are escrowed in an encrypted format. The encryption mechanism 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 by either presenting the associated Identification Credential (for the Subscribers themselves), or by demonstrating that the requestor is a representative of the Organization named in the Certificate.

### **4.12.2. Session Key Encapsulation and Recovery Policy and Practices**

No stipulation.



## 5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

### 5.1. PHYSICAL CONTROLS

#### 5.1.1. Site Location and Construction

Equipment supporting CA operations resides within a physically secured location in geographically separated Apple owned data centers.

#### 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 raised floors, 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. For purposes of backup and recovery, Sub-CA Private Keys, which are stored in encrypted form, are moved to secure storage under dual control. The backups exist in multiple copies in different geographic locations.

## **5.2. PROCEDURAL CONTROLS**

### **5.2.1. Trusted Roles**

Individuals in Trusted Roles have access to or control over cryptographic operations, including access to restricted operations within 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 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 Issuer 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.

### **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 completed background checks 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**

Identity verification is performed on every new Apple employee. Background checks include the following:

- In-person identity verification by means of government-issued photo identification, and
- Documents establishing both identity and employment eligibility, per U.S. Department of Homeland Security Form I-9, Employment Eligibility Verification.

The trustworthiness of individuals in Trusted Roles is verified by performing the additional background check procedures:

- Criminal background check,
- Confirmation of previous employment,
- Check of professional references, and
- Confirmation of the highest or most-relevant educational qualification obtained.

Employees undergo an annual performance review process. Background checks are performed periodically, at least every 5 years, for individuals in Trusted Roles.

### **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**

On a yearly basis, Apple employees receive 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**

Independent contractors are not allowed to serve in Trusted Roles.

### **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 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.
- CA and Subscriber Certificate lifecycle management events, including:
  - Certificate Applications and revocation,
  - All verification activities stipulated in this CPS,





- Date, time, phone number used, persons spoken to, and end results of verification telephone calls if verification is done via telephone call, for EV Certificate validation only,
- Acceptance and rejection of Certificate Applications,
- Issuance of Certificates, and
- Generation of Certificate Revocation Lists and OCSP entries.
- Security events, including:
  - Successful and unsuccessful PKI system access attempts,
  - PKI and security system actions performed,
  - Certificate Problem Reports,
  - 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 seven (7) years. 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 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 data center. Audit logs are archived monthly and retained for the duration of the retention period described in [Section 5.4.3](#).

#### **5.4.6. Audit Collection System (Internal Vs. External)**

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

#### **5.4.7. Notification To Event-Causing Subject**

No stipulation.

#### **5.4.8. Vulnerability Assessments**

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 archives the following types of records:

- The events recorded in [Section 5.4.1](#),
- Certificate lifecycle management events such as Certificate Applications, issuance, and revocation,
- CPS and CPS versions,
- Contracts and agreements,
- System and equipment configurations, modifications, and updates,
- Rejection or acceptance of a Certificate Application,
- 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,
- Sub-CA key generation, backup, and destruction,
- Access to Private Keys for key recovery purposes (Sub-CA and S/MIME Certificates only),
- Export of Private Keys,
- Approval or rejection of a revocation request,
- Appointment of an individual to a Trusted Role,
- Destruction of a cryptographic module,
- Certificate compromise notifications,
- Remedial action taken as a result of violations of physical security, and
- Violations of the CPS.

### **5.5.2. Retention Period for Archive**

Records are retained for at least seven years after any Certificate ceases to be valid.

### **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 data center.



### **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 Public 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](#). Details concerning the creation and storage of archive information are found in [Section 5.5.4](#).

## **5.6. KEY CHANGEOVER**

Towards the end of each Sub-CA’s lifetime, a new CA signing 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 related to Application Software Suppliers’ policy violations. Apple Public CA will address incident reports as outlined in the Mozilla Root Store Policy, [Section 2.4](#), 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 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-CAs 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 of the 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 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 video recorded. A report is produced by the auditors opining on the ceremony.

Ceremonies are conducted in secure facilities described in [Section 5.1](#). 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 Certificates. These Key Pairs are generated by the Subscriber. Before including a Subscriber's key in a TLS 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 are rejected.

Apple Public CA generates Key Pairs used in S/MIME Certificates. The generated keys meet size requirements in [Section 6.1.5](#) and parameters in [Section 6.1.6](#).

#### 6.1.2. Private Key Delivery to Subscriber

For S/MIME Certificates, the Key Pair is provided to the Subscriber using a PKCS#12 file protected by a password with a strength commensurate to the protected key. The PKCS#12 file is distributed separately from the password.

#### 6.1.3. Public Key Delivery to Certificate Issuer

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

#### 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. Algorithm Type and 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 required algorithm type and key sizes specified in the Baseline Requirements [Section 6.1.5.2](#).

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

- Minimum RSA Modulus Size (bits): 2048
- ECC Curve: NIST P-256 and P-384

### 6.1.5.3. Subscriber Certificates

Apple Public CA uses the following algorithms to generate Key Pairs and sign Subscriber Certificates.

#### **TLS Certificates:**

- Digest Algorithm: SHA-256, SHA-384
- Minimum RSA Modulus Size (bits): 2048
- ECC Curve: NIST P-256 and P-384

#### **S/MIME Certificates:**

- Digest Algorithm: SHA-256, SHA-384
- Minimum RSA Modulus Size (bits): 2048
- ECC Curve: NIST P-256 and 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 equal to 3 or more, and that the public exponent is in the range between  $2^{16}+1$  and  $2^{256}-1$ , is an odd number, and has no factors smaller than 752.

For ECC 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](#).

## **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.

### **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](#).

### **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.

### **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**

Operational period for Key Pairs is the same as the operational period for associated Certificates.

Certificates issued by the Apple Public CA are limited to the following operational periods:

- Sub-CA Certificates have a maximum validity period of 15 years.
- TLS Certificates have a maximum validity period of 825 days. After August 31, 2020, the maximum validity period will be 395 days.
- S/MIME Certificates have a maximum validity period of 1125 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 Extensions

Apple Public CA issues Certificates with the extensions shown below. 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).

#### TLS Certificates

TLS Certificates, including EV Certificates, will include the "Required" extensions but may omit "Optional" ones.

Extension	Critical	Required /Optional	Value
Key Usage	Yes	Optional	For RSA keys: Digital Signature, Key Encipherment or For EC Keys: Digital Signature, Key Agreement
Extended Key Usage	No	Required	Server Authentication and/or Client Authentication
Basic Constraints	Yes	Optional	Certification Authority = No
Authority Key Identifier	No	Required	Identifier to Issuer CA's Private Key
Subject Key Identifier	No	Required	Identifier to the subject's Private Key
Certificate Policies	No	Required	Policy OIDs as specified in <a href="#">Section 7.1.6</a>  Policy Qualifiers as specified in <a href="#">Section 7.1.8</a>
CRL Distribution Point	No	Optional	HTTP URL to CRL



Authority Information Access	No	Required (with exception of stapling, see Note 1 below)	HTTP URL to OCSP HTTP URL to Issuer CA
Subject Alternative Name	No	Required	dnsName (minimum of 1, maximum of 100) As specified in <a href="#">Section 7.1.4.3</a> See Notes 2 and 4.
Signed Certificate Timestamp ("SCT")	No	Optional	At least one SCT
Private Subscriber Extension	No	Optional	See Note 3

**Note 1:** The HTTP URL of the Issuing CA's OCSP responder MAY be omitted provided that the Subscriber "staples" OCSP responses for the Certificate in its TLS handshakes [RFC4366].

**Note 2:** Entries in the dnsName are in the "preferred name syntax", as specified in RFC 5280, and thus do not contain underscore characters ("\_")

**Note 3:** Private extension OID must exist within an arc owned by the Subscriber in the Subject DN.

**Note 4:** For EV Certificates, FQDNs with wildcards are not allowed.

### S/MIME Certificates

S/MIME Certificates will include the "Required" extensions but may omit "Optional" ones.

Extension	Critical	Required /Optional	Value
Key Usage	Yes	Optional	Digital Signature, Key Encipherment
Extended Key Usage	No	Required	Email Protection
Basic Constraints	Yes	Optional	Certification Authority = No
Authority Key Identifier	No	Required	Identifier to Issuer CA's Private Key
Subject Key Identifier	No	Required	Identifier to the subject's Private Key
Certificate Policies	No	Required	Policy OIDs as specified in <a href="#">Section 7.1.6</a>  Policy Qualifiers as specified in <a href="#">Section 7.1.8</a>
CRL Distribution Point	No	Optional	HTTP URL to CRL
Authority Information Access	No	Required	HTTP URL to OCSP HTTP URL to Issuer CA



Subject Alternative Name	No	Required	rfc882Name, as specified in <a href="#">Section 7.1.4.3</a>
--------------------------	----	----------	---

### 7.1.3. Algorithm Object Identifiers

Apple Public CA may use these signature algorithms:

Algorithm	Object Identifier
sha256WithRSAEncryption	1.2.840.113549.1.1.11
sha384WithRSAEncryption	1.2.840.113549.1.1.12
ecdsa-with-SHA256	1.2.840.10045.4.3.2
ecdsa-with-SHA384	1.2.840.10045.4.3.3

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

Algorithm	Object Identifier
rsaEncryption	1.2.840.113549.1.1.1
id-ecPublicKey	1.2.840.10045.2.1

### 7.1.4. Name Forms

#### 7.1.4.1. Issuer Information

The Subscriber Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA.

#### 7.1.4.2. Subject Information – Subscriber Certificates

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 with metadata such as ".", "-", and " " (i.e., space) characters are not allowed.

The fields listed below are included depending on the Certificate type:

Field	Certificate Type			Value (Example)
	OV	EV	S/MIME	
Business Category		Required		Type of Subscriber (e.g., Private Organization)
Jurisdiction Country		Required		ISO-3166 country code (e.g., US)
Jurisdiction State		Optional		State Name (e.g., California)
Serial Number		Required		Registration Number for the Organization (e.g., C0806592)



Country (C)	Required	Required	Required	ISO-3166 country code (e.g., US)
State (ST)	Required	Required	Required	State Name (e.g., California)
Locality (L)		Optional		City Name (e.g., Cupertino)
Organization (O)	Required	Required	Required	Subscriber Name (e.g., Apple Inc.)
Organization Unit (OU)	Optional	Optional		Verified Information (e.g., Internal suborganization identifier)
Common Name	Optional	Optional	Required	For TLS: Verified FQDN. See Note 1  For S/MIME: Verified Email Address  For EV Certificates: FQDNs with wildcards are not allowed.

**Note 1:** Entries in the Common Name are in the "preferred name syntax", as specified in RFC 5280, and thus do not contain underscore characters ("\_").

### 7.1.4.3. Subject Alternative Name – Subscribers

Certificates contain the Subject Alternative Name Extension.

For TLS Certificates this extension is populated with the dnsName. Apple Public CA does not currently include ipAddress.

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 FQDN. Internal Names are not allowed.  For EV Certificates, FQDNs with wildcards are not allowed.
rfc822Name			Required	Verified Email Address

### 7.1.4.4. Subject Information - Sub-CA Certificates

Apple Public CA pursues issuance of Sub-CA Certificates that conform to one of the Subject Distinguished Name structures below.





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

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

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

**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 CA issuing 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”.

### 7.1.5. 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. Inclusion of the policy OID indicates adherence to the practices described in this CPS.

Policy OIDs included in Apple Public CA issued Certificates are specified in [Section 1.2](#).

### 7.1.7. Usage of Policy Constraints Extension

No stipulation.

### 7.1.8. Policy Qualifiers Syntax and Semantics

Apple Public CA includes the CPSurl qualifier containing a URL pointing to the CPS outlining the practices for issuance and management.



Certificates may also include the userNotice qualifier with a statement explaining conditions for reliance by a Relying Party. For EV Certificates, the userNotice will always be included.

### 7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

## 7.2. CRL PROFILE

### 7.2.1. Version Number

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

Each CRL contains the following fields:

- **Signature Algorithm:** mirrors the algorithm used by the Issuing CA to sign Certificates
- **Issuer:** matches the Issuing CA's Subject Distinguished Name
- **This Update:** the date of CRL issuance in UTCTime
- **Next Update:** the date of issuance of the next CRL in UTCTime
- **List of Revoked Certificates:**
  - Certificate's Serial Number
  - Revocation date in UTCTime
  - Optionally, a reason code

### 7.2.2. CRL and CRL Entry Extensions

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

CRL Extension	Critical	Required/Optional
CRL Number	No	Required
Authority Key Identifier	No	Required.
CRL Extension	Critical	Required/Optional
Reason Code	No	Optional. If included, the reason code CertificateHold is not allowed.



## 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:** using at least SHA-2 with RSA, or SHA-2 with ECDSA
- **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 pre-Certificates (with no assigned Certificate)
    - **Revoked:** for revoked Certificates
    - **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 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 will be 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.

For TLS Certificates, the auditor will also assess controls to the 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 Trust Service Principles and Criteria for Certification Authorities

### **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.

### **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**

Audit results are communicated to the Apple CA Policy Authority and to others as deemed appropriate based on agreements, regulations or 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 TLS Certificates issued since the last internal audit.

Apple Public CA automatically validates all TLS 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](#).



## **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 privacy policy posted on its website (<https://www.apple.com/legal/privacy>) when handling personal information. Personal information is only disclosed when the disclosure is required by law or when



requested by the subject of the personal information. Such privacy policies conform to applicable local privacy laws.

#### **9.4.2. Information Treated as Private**

Apple Public CA treats all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. Apple protects private information in its possession using a reasonable degree of care and appropriate safeguards. Apple Public CA protects private information using appropriate safeguards and a reasonable degree of care.

#### **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**

Apple Public CA is responsible for securely storing and protecting the private information used for its CA. Apple's employees, agents, and contractors receive training on how to handle confidential information and are contractually obligated to do so.

#### **9.4.5. Notice and Consent To Use Private Information**

Unless otherwise stated in this CPS, the applicable Privacy Policy, or by agreement, Private Information will not be used without the consent of the party to whom that information applies.

#### **9.4.6. Disclosure Pursuant to Judicial or Administrative Process**

Apple Public CA shall be entitled to disclose Confidential/Private Information without notice if, when required to do so by law or regulation or as required to comply with the audit requirements.

#### **9.4.7. Other Information Disclosure Circumstances**

No stipulation.

### **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" is a registered trademark of Apple, Inc. 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.

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 Certificate 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 will be limited to Apple Inc. and its subsidiaries exclusively. Subscribers are solely responsible for any information provided as part of a registration request and for all transactions that use 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 will include 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 (i) 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 (ii) 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 CERTIFICATES 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 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 an EV 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 EV Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) an EV Certificate that has expired or (ii) a revoked EV 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 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.

## **9.10. 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, 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 its terms for all Certificates issued for the remainder of the validity periods of such Certificates until replaced by a newer version.

## **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](#).

Apple will notify Mozilla if:

- Ownership or control of the CA Certificates changes,
- An organization other than the CA obtains control of an unconstrained intermediate certificate, as defined in [Section 5.3.2](#) of the Mozilla Root Store policy, that directly or transitively chains to included Certificate(s),
- Ownership or control of Apple's operations changes, or
- There is a material change in Apple's operations.



## **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**

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

## **9.15. COMPLIANCE WITH APPLICABLE LAW**

This CPS is subject to all applicable laws and regulations, including the United States restrictions on the export of software and cryptography products. Apple is subject to meet the requirements of the European data protection laws, GDPR, and shall take measures to protect against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.



## **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.

### **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.

### **9.16.1. 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	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 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 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 Certificates
		Apple IST CA 8 – G1	0A:48:D5:7C:65:FB:0E:6C:F7:04:A3:64:5F:	TLS Certificates
		Apple Public Client RSA CA 2 – G1	0D:4E:55:BB:BA:DF:A7:8C:14:39:8D:94:AB:ED:	S/MIME 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 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 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 Certificates
DigiCert Global Root G2	DigiCert	Apple Public Client RSA CA 1 – G1	0B:8A:5B:9D:D5:01:A8:87:75:39:9B:9A:04:88:11:A3	S/MIME Certificates
		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 Certificates



Root CA Common Name	Root CA Provider CP	Sub-CA Common Name	Sub-CA Serial Number	Subscriber 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 Certificates
		Apple IST CA 8 – G1	0C:67:62:07:77:A5:AB:C4:BA:53:5D:	TLS 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 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
GeoTrust Global CA	DigiCert	Apple IST CA 2 – G1	00:02:3A:74	TLS 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 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:	S/MIME Certificates
		Apple Public Server RSA CA 11 – G1	5D:FA:BB:95:77:CF:AB:67:1F:C7:DD:FE:D1:CF	TLS Certificates