SSL.com CP/CPS

Certificate Policy and Certification Practice Statement

SSL.com

Version 1.29

March 5, 2026

Table of Contents

1 INTRODUCTION 10

1.1 OVERVIEW - THE SSL.COM CP/CPS 10
1.2 IDENTIFICATION NUMBER AND DOCUMENT NAME 11
1.2.1 DOCUMENT IDENTIFICATION NUMBER 11
1.2.2 DOCUMENT NAME 14
1.2.3 CERTIFICATION PRACTICE STATEMENTS AND SPECIFIC SCENARIOS 15
1.2.4 PROVISION AND AMENDMENT OF SSL.COM CP/CPS 15
1.3 PKI PARTICIPANTS AND THEIR ROLES 15
1.3.1 CERTIFICATION AUTHORITY 19
1.3.2 REGISTRATION AUTHORITY 23
1.3.2.1 ENTERPRISE RAS 24
1.3.2.2 GUIDELINES COMPLIANCE OBLIGATION 25
1.3.3 SUBSCRIBERS 26
1.3.4. RELYING PARTIES 26
1.3.5 OTHER PARTICIPANTS IN THE SSL.COM PKI 27
1.4 CERTIFICATE USAGE 27
1.4.1 ALLOWED CERTIFICATE USAGE 27
1.4.2 PROHIBITED CERTIFICATE USAGE 28
1.5 POLICY ADMINISTRATION 28
1.5.1 ORGANIZATION ADMINISTERING THE SSL.COM CP/CPS 28
1.5.2 CONTACT INFORMATION FOR THE SSL.COM PMA 28
1.5.3 PERSON DETERMINING CP/CPS SUITABILITY FOR THE POLICY 28
1.5.4 CPS APPROVAL PROCEDURES 28
1.6 DEFINITIONS AND ACRONYMS 29
1.6.1 DEFINITIONS 29
1.6.2 ACRONYMS 45
1.6.3 REFERENCES 47
1.6.4 CONVENTIONS 50

2 SSL.COM DOCUMENTS AND REPOSITORY 50

2.1 REPOSITORIES 50
2.2 PUBLICATION OF CERTIFICATION INFORMATION 50
2.2.1 SSL.COM PKI CP/CPS 50
2.2.2 CERTIFICATE REVOCATION LIST AND ON-LINE CERTIFICATE STATUS PROTOCOL 50
2.2.3 SSL.COM CERTIFICATE SUBSCRIBER AGREEMENT 51
2.2.4 SSL.COM RELYING PARTY AGREEMENT AND WARRANTY 51
2.2.5 SSL.COM ROOT AND INTERMEDIATE CERTIFICATES 51
2.2.6 AUDIT REPORTS 51
2.2.7 ADDITIONAL RESOURCES RELATED TO SSL.COM EV CERTIFICATES 51
2.2.8 DISCLOSURE OF VERIFICATION SOURCES 51
2.2.9 OTHER SSL.COM LEGAL DOCUMENTS 52

2.2.10 Documents not included in the SSL.com Repository 52
2.3. Time or Frequency of Publication 52
2.3.1 Frequency of Publication of Certificates 52
2.3.2 Frequency of Publication of CRLs 52
2.3.3 Frequency of Publication of CP/CPS, Terms & Conditions 52
2.3.4 Notification of major changes 53
2.4 Access Controls on Repositories 53

3 NAMING, IDENTIFICATION AND AUTHENTICATION 53

3.1 Naming 53
3.1.1 Type of names 53
3.1.2 Need for names to be meaningful, unambiguous and unique 54
3.1.3 Anonymous, pseudonymous and role-based Certificates 54
3.1.4 Rules for interpreting various name forms 54
3.1.5 Uniqueness of names 54
3.1.6 Recognition, authentication, and role of trademarks 54
3.2 Initial identity validation 55
3.2.1 Method to prove possession of Private Key 55
3.2.2 Authentication of organization and domain identity 56
3.2.3 Authentication of individual identity 80
3.2.4 Non-verified information 82
3.2.5 Validation of authority 82
3.2.6 Criteria for interoperation 83
3.3 Identification and authentication for re-keying 83
3.3.1 Re-keying request by Subscriber 83
3.3.2 Identification and authentication for re-key after revocation 83
3.4 Identification and authentication for revocation requests 84
3.4.1 Identification and authentication for revocation requests by Subscribers 84
3.4.2 Revocation requests by non-Subscribers 84
3.4.3 Identification and authentication for revocation requests by other participants in the SSL.com PKI 84

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 84

4.1 Certificate Application 85
4.1.1 Who may submit a certificate application 85
4.1.2 Enrollment process and responsibilities 86
4.2 Certificate application processing 87
4.2.1 Performing identification and authentication functions 87
4.2.2 Approval or rejection of certificate applications 89
4.2.3 Time to process certificate applications 91
4.2.4 Certificate Authority Authorization (CAA) 91
4.2.5 Re-issuance Requests 92
4.3 Certificate issuance 92
4.3.1 CA actions during certificate issuance 92
4.3.2 Notification to Subscriber by the CA of issuance of Certificate 93

4.4 CERTIFICATE ACCEPTANCE 94
4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE 94
4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA 94
4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES 94
4.5 KEY PAIR AND CERTIFICATE USAGE 94
4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE 94
4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE 95
4.6 CERTIFICATE RENEWAL 95
4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL 95
4.6.2 WHO MAY REQUEST RENEWAL 96
4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS 96
4.6.4 NOTIFICATION OF RENEWED CERTIFICATE ISSUANCE TO SUBSCRIBER 96
4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE 96
4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA 96
4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES 96
4.7 CERTIFICATE RE-KEY 97
4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY 97
4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY 98
4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS 98
4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER 98
4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE 99
4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA 99
4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES 99
4.8 CERTIFICATE MODIFICATION 99
4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION 99
4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION 99
4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS 99
4.8.4 NOTIFICATION OF MODIFIED CERTIFICATE ISSUANCE TO SUBSCRIBER 100
4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE 100
4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA 100
4.8.7 NOTIFICATION OF MODIFIED CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES 100
4.9 CERTIFICATE REVOCATION AND SUSPENSION 100
4.9.1 CIRCUMSTANCES FOR REVOCATION 100
4.9.2 WHO CAN REQUEST REVOCATION 103
4.9.3 PROCEDURE FOR REVOCATION REQUEST 103
4.9.4 REVOCATION REQUEST GRACE PERIOD 105
4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST 106
4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES 107
4.9.7 CRL ISSUANCE FREQUENCY 107
4.9.8 MAXIMUM LATENCY FOR CRLS 108
4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY 108
4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS 109
4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE 110
4.9.12 SPECIAL REQUIREMENTS REGARDING KEY COMPROMISE 110
4.9.13 CIRCUMSTANCES FOR SUSPENSION 110
4.9.14 WHO CAN REQUEST SUSPENSION 110
4.9.15 PROCEDURE FOR SUSPENSION REQUEST 110
4.9.16 LIMITS ON SUSPENSION PERIOD 110

4.10 CERTIFICATE STATUS SERVICES 110
4.10.1 OPERATIONAL CHARACTERISTICS 111
4.10.2 SERVICE AVAILABILITY 111
4.10.3 OPTIONAL FEATURES 111
4.11 END OF SUBSCRIPTION 111
4.12 KEY ESCROW AND RECOVERY 111
4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES 112
4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES 112

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 112

5.1 PHYSICAL CONTROLS 112
5.1.1 SITE LOCATION AND CONSTRUCTION 112
5.1.2 PHYSICAL ACCESS 112
5.1.3 POWER AND AIR CONDITIONING 112
5.1.4 WATER EXPOSURES 113
5.1.5 FIRE PREVENTION AND PROTECTION 113
5.1.6 MEDIA STORAGE 113
5.1.7 WASTE DISPOSAL 113
5.1.8 OFF-SITE BACKUP 113
5.2 PROCEDURAL CONTROLS 113
5.2.1 TRUSTED ROLES 113
5.2.2 NUMBER OF PERSONS REQUIRED PER TASK 114
5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE 115
5.2.4 ROLES REQUIRING SEPARATION OF DUTIES 115
5.3 PERSONNEL CONTROLS 115
5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS 115
5.3.2 BACKGROUND CHECK PROCEDURES 115
5.3.3 TRAINING REQUIREMENTS 115
5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS 116
5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE 116
5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS 116
5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS 116
5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL 117
5.4 AUDIT LOGGING PROCEDURES 117
5.4.1 TYPES OF EVENTS RECORDED 117
5.4.2 FREQUENCY OF PROCESSING AUDIT LOG 119
5.4.3 RETENTION PERIOD FOR AUDIT LOG 119
5.4.4 PROTECTION OF AUDIT LOG 120
5.4.5 AUDIT LOG BACKUP PROCEDURES 120
5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL) 120
5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT 120
5.4.8 VULNERABILITY ASSESSMENTS 120
5.5 RECORDS ARCHIVAL 121
5.5.1 TYPES OF RECORDS ARCHIVED 121
5.5.2 RETENTION PERIOD FOR ARCHIVE 121
5.5.3 PROTECTION OF ARCHIVE 122

5.5.4 Archive backup procedures 122
5.5.5 Requirements for time-stamping of records 122
5.5.6 Archive collection system (internal or external) 123
5.5.7 Procedures to obtain and verify archive information 123
5.6 Key changeover 123
5.7 Compromise and disaster recovery 123
5.7.1 Incident and compromise handling procedures 123
5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted 125
5.7.3 Recovery Procedures After Key Compromise 125
5.7.4 Business continuity capabilities after a disaster 125
5.8 CA or RA termination 125

6 TECHNICAL SECURITY CONTROLS 126

6.1 Key Pair Generation and Installation 126
6.1.1 Key Pair Generation 126
6.1.2. Private Key Delivery to Subscriber 127
6.1.3 Public key delivery to certificate issuer 128
6.1.4 CA Public Key delivery to Relying Parties 128
6.1.5 Key sizes 128
6.1.6 Public key parameters generation and quality checking 130
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 130
6.2 Private Key Protection and Cryptographic Module Engineering Controls 130
6.2.1 Cryptographic module standards and controls 131
6.2.2 Private key (n out of m) multi-person control 131
6.2.3 Private key escrow 131
6.2.4 Private key backup 131
6.2.5 Private key archival 131
6.2.6 Private key transfer into or from a cryptographic module 131
6.2.7 Private key storage on cryptographic module 132
6.2.8 Method of activating Private Key 135
6.2.9 Method of deactivating Private Key 136
6.2.10 Method of destroying Private Key 136
6.2.11 Cryptographic Module Rating 136
6.3 Other aspects of Key Pair management 136
6.3.1 Public key archival 136
6.3.2 Certificate operational periods and Key Pair usage periods 136
6.4 Activation data 138
6.4.1 Activation Data Generation and Installation 138
6.4.2 Activation data protection 138
6.4.3 Other aspects of activation data 138
6.5 Computer security controls 139
6.5.1 Specific computer security technical requirements 139
6.5.2 Computer security rating 139
6.6 Life cycle technical controls 139
6.6.1 System development controls 139
6.6.2 Security management controls 140

6.6.3 Life cycle security controls 140
6.7 Network security controls 140
6.8 Time-stamping 141

7 CERTIFICATE, CRL, AND OCSP PROFILES 142

7.1 Certificate Profiles 142
7.1.1 Version Numbers 142
7.1.2 Certificate Content and Extensions 142
7.1.3 Algorithm object identifiers 150
7.1.4 Name forms 155
7.1.5 Name Constraints 166
7.1.6 Certificate Policy object identifier 167
7.1.7 Usage of Policy Constraints extension 171
7.1.8 Policy qualifiers syntax and semantics 171
7.1.9 Processing semantics for the critical Certificate Policies extension 171
7.2 CRL Profile 171
7.2.1 Version Numbers 171
7.2.2 CRL and CRL Entry Extensions 171
7.3 OCSP Profile 173
7.3.1 Version Numbers 174
7.3.2 OCSP Extensions 174

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 174

8.1 Frequency or circumstances of assessment 174
8.2 Identity/qualifications of assessor 174
8.3 Assessor's relationship to assessed entity 175
8.4 Topics covered by assessment 175
8.4.1 CA assessment 175
8.4.2 Signing Service assessment 176
8.4.3 Timestamp Authority assessment 176
8.5 Actions taken as a result of deficiency 177
8.6 Communication of results 177
8.7 Self-Audits 177

9 OTHER BUSINESS AND LEGAL MATTERS 178

9.1 Fees 178
9.1.1 Certificate issuance or renewal fees 178
9.1.2 Certificate access fees 178
9.1.3 Revocation or status information access fees 178
9.1.4 Fees for other services 179
9.1.5 Refund policy 179
9.2 Financial responsibility 179
9.2.1 Insurance coverage 179

9.2.2 Other assets 179
9.2.3 Insurance or warranty coverage for end-entities 179
9.3 Confidentiality of business information 179
9.3.1 Scope of Confidential Information 179
9.3.2 Information Not Within the Scope of Confidential Information 180
9.3.3 Responsibility to Protect Confidential Information 180
9.4 Privacy of personal information 180
9.4.1 Privacy plan 180
9.4.2 Information treated as private 180
9.4.3 Information not deemed private 180
9.4.4 Responsibility to protect private information 181
9.4.5 Notice and consent to use private information 181
9.4.6 Disclosure pursuant to judicial or administrative process 181
9.4.7 Other information disclosure circumstances 181
9.5 Intellectual property rights 181
9.6 Representations and warranties 181
9.6.1 CA representations and warranties 181
9.6.2 RA representations and warranties 184
9.6.3 Subscriber representations and warranties 185
9.6.4 Relying party representations and warranties 186
9.6.5 Representations and warranties of other participants 187
9.7 Disclaimers of warranties 187
9.8 Limitations of liability 188
9.9 Indemnities 188
9.9.1 Indemnification by CAs 188
9.9.2 Indemnification by Subscribers 189
9.9.3 Indemnification by Relying Parties 189
9.10 Term and termination 189
9.10.1 Term 189
9.10.2 Termination 189
9.10.3 Effect of termination and survival 189
9.11 Individual notices and communications with participants 190
9.12 Amendments 190
9.12.1 Procedure for amendment 190
9.12.2 Notification mechanism and period 190
9.12.3 Circumstances under which OID must be changed 190
9.13 Dispute resolution provisions 190
9.14 Governing law 191
9.15 Compliance with applicable law 191
9.16 Miscellaneous provisions 191
9.16.1 Entire agreement 191
9.16.2 Assignment 191
9.16.3 Severability 191
9.16.4 Enforcement (attorneys' fees and waiver of rights) 192
9.16.5 Force Majeure 192
9.17 Other provisions 192

ANNEX A - SSL.COM COMMONLY USED CERTIFICATE PROFILES 192

1 INTRODUCTION

SSL.com is a Certification Authority (CA) that issues digital Certificates to entities and individuals according to the SSL.com Certificate Policy and Certification Practice Statement (CP/CPS). SSL.com performs Public Key life-cycle functions that include receiving certificate requests, issuing, revoking and renewing digital Certificates. In addition, SSL.com maintains and publishes the Certificate Revocation Lists (CRLs) for participants within the SSL.com Public Key Infrastructure (PKI).

1.1 Overview - The SSL.com CP/CPS

This document incorporates the SSL.com Certificate Policy (CP) and SSL.com Certification Practice Statement (CPS) into a single document, henceforth referred to as the SSL.com CP/CPS. It sets forth the business, legal, and technical requirements, principles and practices surrounding digital certification services provided by SSL.com.

This CP/CPS conforms to the current version of guidelines adopted by the Certification Authority/Browser Forum ("CAB Forum") and published at (https://www.cabforum.org). In particular:

- Publicly trusted TLS Certificates are issued and managed per the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates ("Baseline Requirements"). The Guidelines for Extended Validation Certificates ("EV Guidelines") are observed in the issuance of Extended Validation ("EV") TLS Certificates.
- Code Signing and Extended Validation Code Signing ("EV Code Signing") Certificates are issued and managed per the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates ("Code Signing Baseline Requirements").
- Email Protection ("S/MIME") Certificates are issued and managed per the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates ("S/MIME Baseline Requirements").
- Mark Certificates ("MC") are issued and managed per the Minimum Security Requirements for Issuance of Mark Certificates ("MC Requirements") maintained by the AuthIndicators Working Group and published at https://bimigroup.org/supporting-documents/.
- Issuance of SSL.com certificates to NAESB Subscribers observes the North American Energy Standards Board (NAESB) Accreditation Requirements for Authorized Certificate Authorities.
- SSL.com time-stamping services follow IETF RFC 3161.

The SSL.com CP/CPS uses the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647). In accordance with RFC 3647, this CP/CPS is organized using numbered paragraphs. Items that do not currently apply to SSL.com PKI will have the statement "Not applicable" or "No stipulation".

SSL.com's Policy Management Authority (PMA) will continuously keep track of changes in SSL.com policies and applicable guidelines, incorporate required changes before their effective dates, and update this CP/CPS accordingly. In the event of any inconsistency between this CP/CPS and the guidelines given above, the relevant CAB Forum publication shall take precedence over this document.

This CP/CPS applies to all entities and individuals utilizing SSL.com certification services.

Other important documents also apply to SSL.com certification services. These include public documents (such as agreements with Subscribers and other SSL.com customers, Relying Party agreements, and the SSL.com privacy policy) and private documents governing internal operations.

1.2 Identification Number and Document Name

1.2.1 Document Identification Number

The OID assigned to SSL.com by IANA is:

iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) SSL.com (38064)

A special OID arc has been allocated by SSL.com for Certificate Policy / Certification Practice Statement:

iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) SSL.com (38064) certificationServicesProvision (1) certificatePolicyCertificationPracticeStatement (1)

The globally unique Identification Number (OID) of the SSL.com CP/CPS (this document) is:

1.3.6.1.4.1.38064.1.1.1.29

OID Arc	Description
1.3.6.1.4.1.**38064**	Identification Number (OID) of SSL.com, registered to IANA (www.iana.org)
1.3.6.1.4.1.38064.**1**	Certification Services Provision
1.3.6.1.4.1.38064.1.**1**	Certificate Policy / Certification Practice Statement
1.3.6.1.4.1.38064.1.1.**1.29**	First and Second number of the version identifying this document

Version Control

Version	**Date**	**Information**
1.0	**July 1 2016**	First release
1.1	**September 1, 2016**	Added support for EV Code Signing Certificates
1.2	**June 13, 2017**	Updated for BRs 1.4.8

Version	Date	Information
1.2.1	**June 21, 2017**	Minor revisions
1.3	**December 28, 2017**	Applied changes introduced in BRs 1.5.4, EV Guidelines 1.6.7, EV Code Signing Guidelines 1.4, Minimum Requirements for Code Signing Certificates 1.1. Also, clarified 9.12.1, added Microsoft Kernel Mode Code Signing OID.
1.4	**May 25, 2018**	Added requirements for NAESB Policies. Removed Microsoft Kernel Mode Code Signing OID and profiles.
1.5	**October 30, 2018**	Applied changes introduced in BRs 1.6.0 and EV Guidelines 1.6.8.
1.5.1	**December 13, 2018**	Minor update of CP/CPS OID in §7.1.6 to link to §1.2.1
1.6	**May 20, 2019**	Applied changes related to NAESB Server Certificates and per BRs 1.6.4. Custom SSL.com OIDs were added in §7.1.6. Annex A was updated with the most commonly used Certificate Profiles.
1.7	**Sep 20, 2019**	Updated requirements to fulfill Adobe Root Program. Annex A was updated with the most commonly used Certificate Profiles.
1.8	**Oct 16, 2019**	Applied changes introduced in BRs 1.6.6 and EV Guidelines 1.7.0. Clarified identity validation for Document Signing Certificates.
1.9	**May 29, 2020**	Applied changes introduced in BRs 1.7.0 and EV Guidelines 1.7.2. Set maximum certificate lifetime for TLS Certificates to 398 days on and after Sep 1, 2020. Clarified the term “Certificate Problem Report”.
1.10	**Sep 30, 2020**	Applied changes introduced in BRs 1.7.2 and EV Guidelines 1.7.3.
1.11	**Feb 16, 2021**	Applied changes introduced in BRs 1.7.3, EV Guidelines 1.7.4 and the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates 2.1. Updated language for: managing keys on behalf of Subscribers, email address validation, validation of Natural Persons associated with Legal Entities, revocation requests from Governmental or regulatory authorities.
1.12	**Apr 9, 2021**	Describe EV Certificate re-issuance process. Add Certum EV Code Signing Policy Identifier.
1.13	**Jun 30, 2021**	Applied changes introduced in BRs 1.7.6, EV Guidelines 1.7.6 and the Baseline Requirements for the Issuance and

Version	Date	Information
		Management of Publicly-Trusted Code Signing Certificates 2.3. Language improvements and clarifications. Update event logging and records archival policy. Update 4.9.12 with methods to demonstrate private key compromise. Additional changes: Stop using Wildcard Domain Validation via agreed-upon change to a web site; Sunset the CAA exception for DNS Operator.
1.14	**Oct 22, 2021**	Applied changes introduced in BRs 1.8.0, EV Guidelines 1.7.8 and the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates 2.5.
1.15	**Mar 30, 2022**	Applied changes introduced in BRs 1.8.2 and the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates 2.7. Update based on ballot SC53 to deprecate SHA-1 in OCSP responses. Update maximum validity period for S/MIME Certificates. Added policy OID for Time-stamping Certificate for Document Signing Trust. Allowed IP validation methods 3.2.2.5.6, 3.2.2.5.7. Updated WebTrust criteria.
1.16	**Sep 14, 2022**	Applied changes introduced in TLS BRs 1.8.4, TLS EV Guidelines 1.7.9, Mozilla Root Store Policy 2.8 and Chrome Root Program Policy 1.1. Updated identity proofing provisions. Added fingerprints of the new 2022 Root-CAs.
1.17	**May 11, 2023**	Improved validation related provisions, in particular with reference to TLS EV Guidelines per Mozilla's remarks. Updated log retention period to align with TLS BRs.
1.18	**August 22, 2023**	Applied changes introduced in Code Signing BRs 3.0.0, update log retention period. Improved references to EV Guidelines. Improved description of validation of authority. Improved description of authentication of individual identity for server certificates. Applied changes introduced in TLS BRs 1.8.7, TLS EV Guidelines 1.8.0, Code Signing BRs 3.2, S/MIME BRs v1.0.0, Mozilla Root Store Policy 2.8.1 and Chrome Root Program Policy 1.4.
1.19	**September 19, 2023**	Applied changes introduced in S/MIME BRs v1.0.1, Code Signing BRs 3.3, TLS BRs 2.0.0, TLS BRs 2.0.1. Added provisions for Test Document Signing Certificates. Other improvements and clarifications.
1.20	**April 18, 2024**	Compliance with Minimum Requirements for Verified Mark Certificates. Support for Domain Validation method ACME

Version	Date	Information
		ALPN. Applied changes introduced in TLS BRs 2.0.2, TLS EV Guidelines 1.8.1, CS BRs 3.7, S/MIME BRs 1.0.3, Mozilla Root Store Policy 2.9.
1.21	**September 13, 2024**	Added Entrust's CAA domain names. Added VMC Root CA Certificates. Changed validity period from 397 to 398 days. Removal of CERTUM EV policy OIDs. Added support for Domain Validation method 3.2.2.4.13. Added sampling of S/MIME Certificates in quarterly internal audits. Updated §3.1.2 to align with S/MIME BRs.
1.22	**December 13, 2024**	Applied changes introduced in TLS BRs 2.0.3 to 2.0.8, TLS EV 2.0.0 and 2.0.1, CS BRs 3.8 and 3.9, S/MIME BRs 1.0.5 to 1.0.6. Other improvements and clarifications.
1.23	**March 4, 2025**	Applied changes introduced in TLS BRs 2.0.9 to 2.1.0, S/MIME BRs 1.0.3.
1.24	**April 28, 2025**	Applied changes introduced in TLS BRs 2.1.1 to 2.1.3, S/MIME BRs 1.0.4 and S/MIME BRs 1.0.7 to 1.0.8. Blocking Address and Routing Parameter Area Names. Added support for `id-kp-documentSigning` according to RFC 9336. Other improvements and clarifications.
1.25	**July 2, 2025**	Compliance with Minimum Requirements for Common Mark Certificates. Other formatting improvements and clarifications.
1.26	**July 31, 2025**	Applied changes introduced in TLS BRs 2.1.4 and 2.1.5, S/MIME BRs 1.0.10.
1.27	**November 7, 2025**	Applied changes introduced in TLS BRs 2.1.7, NCSSR 2.0.5.
1.28	**February 13, 2026**	Applied changes introduced in TLS BRs 2.1.6, 2.2.0 and 2.2.2, CS BRs 3.10.0, S/MIME BRs 1.0.11 and 1.0.12. Support for Government Mark Certificates. Other improvements and clarifications.
1.29	**March 5, 2026**	SSL.com legal address update. Addition of VC Root CAs. Other improvements and clarifications.

1.2.2 Document Name

This document is the SSL.com CP/CPS and constitutes the documentation and regulatory frame for SSL.com's PKI. This document incorporates both the Certificate Policy and the Certification Practice Statement for SSL.com's operations. In abbreviation, it will be referred as the "SSL.com CP/CPS" or "CP/CPS".

1.2.3 Certification Practice Statements and specific scenarios

Should the need arise to follow any additional practice beyond what is outlined in this CP/CPS, a corresponding alternate certification practice statement (alternate CPS) will be created and referenced in this document. The resulting document(s) will be a separate CPS that applies to specific cases. The new alternate CPS will describe particular cases where it applies, the different procedures that will apply in those particular cases, and the specific sections of the SSL.com CP/CPS which the alternate CPS modifies or supersedes.

For NAESB Subscribers, SSL.com shall follow all procedures (including those related to verification, issuance, re-issuance and revocation, log archiving and any other NAESB-specific requirements) as described in the relevant WEQ and related NAESB guidelines (see §1.6.3). Any certificate issued to NAESB Subscribers SHALL incorporate the appropriate OID for the level of assurance of that certificate (see §7.1.6).

1.2.4 Provision and amendment of SSL.com CP/CPS

The provisions of the SSL.com CP/CPS, as amended from time to time, are publicly available via the SSL.com repository. Amendments to this document will be made in accordance with Sections 1.5 and 9.12.

1.3 PKI participants and their roles

The roles which comprise SSL.com's PKI include Certification Authorities (CAs), Registration Authorities (RAs), Subscribers and Relying Parties.

- A Certification Authority (CA) is the entity responsible for issuing Certificates.
- A CA utilizes at least one Registration Authority (RA) for identifying, authenticating and managing a Subscriber's certificate request information.
- A Subscriber is any party which has been issued a certificate by SSL.com.
- A Relying Party is any party who performs transactions, communications and/or functions that rely on a certificate issued by SSL.com.

Also refer to §1.6.1 for definition of these terms.

The diagrams below indicate the relationship between these components:

SSL.com Original CA Hierarchy

Figure 1: SSL.com Original CA Hierarchy

Figure 2: SSL.com Original EV CA Hierarchy

Figure 3: SSL.com Original ECC CA Hierarchy

Figure 4: SSL.com Original EV ECC CA Hierarchy

SSL.com 2022 Root CA Hierarchy

Figure 5: 2022 SSL.com CA Hierarchy

Figure 6: 2022 SSL.com EV CA Hierarchy

Figure 7: 2022 SSL.com ECC CA Hierarchy

Figure 8: 2022 SSL.com EV ECC CA Hierarchy

Other Root CA Hierarchy effective March 6, 2026

Figure 9: SecureTrust CA Hierarchy

1.3.1 Certification Authority

Within the SSL.com PKI hierarchy, SSL.com functions as both the Root CA and as an Issuing CA.

1.3.1.1 Root CA role

In its role as a Root CA, SSL.com makes available to Subscribers a dedicated root hierarchy to ensure the integrity and uniqueness of Certificates issued through the SSL.com PKI. Starting in 2022, SSL.com created separate hierarchies per certificate type as follows:

- TLS Root hierarchy to be used for server TLS Certificates
- Client Root hierarchy to be used for client authentication and email (S/MIME) Certificates
- Code Signing Root hierarchy to be used for Code Signing and Time-stamping Certificates associated with Code Signing
- Document Signing Root hierarchy to be used for Document Signing and Time-stamping Certificates associated with Document Signing.

The following Root CA Certificates are governed by this CP/CPS:

- SSL.com TLS RSA Root CA 2022
    - Serial Number: 6FBEDAAD73BD0840E28B4DBED4F75B91
    - SHA-1 Fingerprint: EC:2C:83:40:72:AF:26:95:10:FF:0E:F2:03:EE:31:70:F6:78:9D:CA
    - download PEM format
    - download DER format
- SSL.com TLS ECC Root CA 2022

    - Serial Number: 1403F5ABFB378B17405BE243B2A5D1C4
    - SHA-1 Fingerprint: 9F:5F:D9:1A:54:6D:F5:0C:71:F0:EE:7A:BD:17:49:98:84:73:E2:39
    - download PEM format
    - download DER format
- SSL.com Client RSA Root CA 2022
    - Serial Number: 76AFEE88931545B650539B809CA4DF9A
    - SHA-1 Fingerprint: AA:59:70:E5:20:32:9F:CB:D0:D5:79:9F:FB:1B:82:1D:FD:1F:79:65
    - download PEM format
    - download DER format
- SSL.com Client ECC Root CA 2022
    - Serial Number: 76F8481EAEF03C701FE03F25540183D5
    - SHA-1 Fingerprint: 80:7B:1D:9D:65:72:3D:C7:56:F9:EC:C5:00:83:49:F6:F2:AC:F4:86
    - download PEM format
    - download DER format
- SSL.com Code Signing RSA Root CA 2022
    - Serial Number: 1097C49C8C254328BBA6E8B99BAB4FA1
    - SHA-1 Fingerprint: D4:69:52:84:CD:17:98:D9:CB:16:99:46:4C:06:49:94:C4:E2:BB:FD
    - download PEM format
    - download DER format
- SSL.com Code Signing ECC Root CA 2022
    - Serial Number: 6E8EE45B104CC90C7EB4D8888FE5EC64
    - SHA-1 Fingerprint: 0D:9E:9A:B2:07:65:A8:9E:D9:CD:8D:F2:C7:A6:3B:C7:74:95:EF:31
    - download PEM format
    - download DER format
- SSL.com Document Signing RSA Root CA 2022
    - Serial Number: 50D0D50DADDD017E55D169903BD21F46
    - SHA-1 Fingerprint: 2F:68:6D:C8:D4:E3:95:53:ED:32:93:8E:63:57:13:3B:B7:D9:91:0C
    - download PEM format
    - download DER format
- SSL.com Document Signing ECC Root CA 2022
    - Serial Number: 5A88B596192224E56A90CA0BBAD83A2B
    - SHA-1 Fingerprint: 3C:C1:A6:83:FF:E6:68:36:49:1A:F3:6B:E1:D3:FE:0A:37:F5:9D:AE
    - download PEM format

    - download DER format
- SSL.com SSL.com Root Certification Authority RSA
    - Serial Number: 7B2C9BD316803299
    - SHA-1 Fingerprint: B7:AB:33:08:D1:EA:44:77:BA:14:80:12:5A:6F:BD:A9:36:49:0C:BB
    - download PEM format
    - download DER format
- SSL.com Root Certification Authority ECC
    - Serial Number: 75E6DFCBC1685BA8
    - SHA-1 Fingerprint: C3:19:7C:39:24:E6:54:AF:1B:C4:AB:20:95:7A:E2:C3:0E:13:02:6A
    - download PEM format
    - download DER format
- SSL.com EV Root Certification Authority RSA R2
    - Serial Number: 56B629CD34BC78F6
    - SHA-1 Fingerprint: 74:3A:F0:52:9B:D0:32:A0:F4:4A:83:CD:D4:BA:A9:7B:7C:2E:C4:9A
    - download PEM format
    - download DER format
- SSL.com EV Root Certification Authority ECC
    - Serial Number: 2C299C5B16ED0595
    - SHA-1 Fingerprint: 4C:DD:51:A3:D1:F5:20:32:14:B0:C6:C5:32:23:03:91:C7:46:42:6D
    - download PEM format
    - download DER format
- SSL.com VMC Root 2024 RSA
    - Serial Number: 70946FAEBEB3CCE0D86FB876778061CB
    - SHA-1 Fingerprint: BB:AD:CB:97:B9:6A:78:E2:24:11:EA:2C:7E:2A:F4:5A:97:46:57:C5
    - download PEM format
    - download DER format
- SSL.com VMC Root 2024 ECC
    - Serial Number: 1147C16A2D3F4AF7675D65E5C1ACAD8E
    - SHA-1 Fingerprint: 2C:8F:C6:88:3D:06:F1:6C:1E:DA:1A:20:65:A6:79:CB:EF:75:FC:E6
    - download PEM format
    - download DER format

Other Root CA Certificates effective March 6, 2026

- XRamp Global Certification Authority
  - Serial Number: 50946CEC18EAD59C4DD597EF758FA0AD
  - SHA-1 Fingerprint: B8:01:86:D1:EB:9C:86:A5:41:04:CF:30:54:F3:4C:52:B7:E5:58:C6
  - download PEM format
  - download DER format

- SecureTrust CA
  - Serial Number: 0CF08E5C0816A5AD427FF0EB271859D0
  - SHA-1 Fingerprint: 87:82:C6:C3:04:35:3B:CF:D2:96:92:D2:59:3E:7D:44:D9:34:FF:11
  - download PEM format
  - download DER format

- Secure Global CA
  - Serial Number: 075622A4E8D48A894DF413C8F0F8EAA5
  - SHA-1 Fingerprint: 3A:44:73:5A:E5:81:90:1F:24:86:61:46:1E:3B:9C:C4:5F:F5:3A:1B
  - download PEM format
  - download DER format

- Trustwave Global Certification Authority
  - Serial Number: 05F70E86DA49F346352EBAB2
  - SHA-1 Fingerprint:
  2F:8F:36:4F:E1:58:97:44:21:59:87:A5:2A:9A:D0:69:95:26:7F:B5
  - download PEM format
  - download DER format

- Trustwave Global ECC P256 Certification Authority
  - Serial Number: 0D6A5F083F285C3E5195DF5D
  - SHA-1 Fingerprint: B4:90:82:DD:45:0C:BE:8B:5B:B1:66:D3:E2:A4:08:26:CD:ED:42:CF
  - download PEM format
  - download DER format

- Trustwave Global ECC P384 Certification Authority
  - Serial Number: 08BD85976C9927A48068473B
  - SHA-1 Fingerprint: E7:F3:A3:C8:CF:6F:C3:04:2E:6D:0E:67:32:C5:9E:68:95:0D:5E:D2
  - download PEM format
  - download DER format

1.3.1.2 Issuing CA role

In its role as an issuing CA, SSL.com performs functions associated with Public Key operations that include:

- Receiving requests for Certificates
- Issuing, revoking and renewing Certificates

- Maintenance, issuance, and publication of a definitive Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) as resources for users of Certificates related to the SSL.com PKI.

SSL.com intends to use the following issuing CA structure under the "2022" TLS Root hierarchy:

- "global" subCA for DV TLS
- "global" subCA for OV TLS
- "global" subCA for IV TLS
- "global" subCA for EV TLS
- "branded" subCA per customer for DV/OV/IV/EV.

1.3.1.3 General CA roles

In its capacity as a CA, SSL.com:

- Conforms its operations to the SSL.com CP/CPS
- Issues and publishes Certificates in a timely manner
- Revokes Certificates upon receipt of a valid and authorized request, or on its own initiative when circumstances warrant
- Notifies Certificate holders of the imminent expiry of their Certificates.

1.3.2 Registration Authority

Any CA utilizes at least one RA for identifying, authenticating and managing a Subscriber's certificate request information. Depending on the type of CA, registration requirements of this CA and the assurance level, a Subscriber may need to perform specific registration operations (for example face-to-face proof of identity, inquiries to official local government list of commercial organizations, etc). These operations are performed by RAs operated under the supervision of SSL.com, utilizing trusted personnel and/or trustworthy systems providing equivalent assurance. SSL.com operates the central RA of the SSL.com hierarchy.

With the exception of sections §3.2.2.4 and §3.2.2.5, SSL.com MAY delegate the performance of all or any part of these requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of §3.2 of this CP/CPS.

Before SSL.com authorizes a Delegated Third Party to perform a delegated function, SSL.com SHALL contractually require the Delegated Third Party to:

1. Meet the qualification requirements of §5.3.1, when applicable, to the delegated function;
2. Retain documentation in accordance with §5.5.2;
3. Comply with (a) the SSL.com CP/CPS or (b) the Delegated Third Party's (SSL.com-approved) CP/CPS; and

4. Abide by the other provisions (i.e. CAB Forum Requirements designated in §1.1, Contract between SSL.com and Delegated Third Parties) that are applicable to the delegated function.

SSL.com MAY delegate the performance of all or any part of EV Validation to an Affiliate or a Registration Authority (RA) or subcontractor, provided that the process employed fulfills all of the requirements of the EV Guidelines. Affiliates and/or RAs must comply with the qualification requirements of Sections §5.2 and §5.3.

SSL.com SHALL verify that any Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of §5.3 and the document retention and event logging requirements of §5.4.

1.3.2.1 Enterprise RAs

For TLS Server Certificates: SSL.com MAY designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization. SSL.com SHALL NOT accept certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. SSL.com SHALL confirm that the requested Fully-Qualified Domain Name(s) are within the Enterprise RA's verified Domain Namespace.
2. If the certificate request includes a Subject name of a type other than a Fully-Qualified Domain Name, SSL.com SHALL confirm that the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, SSL.com SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are affiliated (see §3.2) or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested Subject FQDN falls within the Domain Namespace of ABC Co.'s Registered Domain Name.

SSL.com SHALL impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA.

For EV TLS and Code Signing Certificates: SSL.com MAY contractually authorize the Subject of a specified Valid EV Certificate to perform the RA function and authorize SSL.com to issue additional EV Certificates at third and higher domain levels that are contained within the domain of the original EV Certificate (also known as an Enterprise EV Certificate). In such case, the Subject shall be considered an Enterprise RA, and the following requirements SHALL apply:

1. An Enterprise RA SHALL NOT authorize SSL.com to issue an Enterprise EV Certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA;
2. In all cases, the Subject of an Enterprise EV Certificate must be an organization verified by SSL.com in accordance with the EV Guidelines;
3. SSL.com must impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by the Enterprise RA;

4. The Final Cross-Correlation and Due Diligence requirements of the EV Guidelines may be performed by a single person representing the Enterprise RA; and
5. The audit requirements of §8.4 SHALL apply to the Enterprise RA, except in the case where SSL.com maintains control over the Root CA Private Key or Subordinate CA Private Key used to issue the Enterprise EV Certificates, in which case, the Enterprise RA may be exempted from the audit requirements.
6. SSL.com does NOT contractually authorize the Subject of a specified Valid EV Code Signing Certificate to perform the RA function and authorize SSL.com to issue additional EV Code Signing Certificates.

For S/MIME Certificates: SSL.com MAY delegate to an Enterprise Registration Authority (RA) to verify Certificate Requests for Subjects within the Enterprise RA's own organization. SSL.com SHALL NOT accept Certificate Requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. If the Certificate Request is for a `Mailbox-validated`, `Organization-validated`, or `Sponsor-validated` profile, SSL.com SHALL confirm that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with §3.2.2.9.1 or §3.2.2.9.3.
2. SSL.com SHALL confirm that the `subject:organizationName` name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, SSL.com SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are Affiliated as defined in §3.2 or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested email domain falls within the subdomains of ABC Co.'s Registered Domain Name.

SSL.com SHALL impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA in accordance with §8.4.

An Enterprise RA MAY also submit Certificate Requests using the `Mailbox-validated` profile for users whose email domain(s) are not under the delegated organization's authorization or control. In this case, SSL.com SHALL confirm that the mailbox holder has control of the requested Mailbox Address(es) in accordance with §3.2.2.9.2 or §3.2.2.9.4

1.3.2.2 Guidelines Compliance Obligation

In all cases, SSL.com contractually obligates each Affiliate, RA, subcontractor, and Enterprise RA to comply with all applicable requirements in this CP/CPS and to perform them as required of SSL.com itself. SSL.com shall enforce these obligations and internally audit each Affiliate's, RA's, subcontractor's, and Enterprise RA's compliance with this CP/CPS on an annual basis.

1.3.3 Subscribers

A Subscriber is any natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

1.3.3.1 Applicants

An Applicant is any natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Prior to verification of identity and issuance of a certificate, any requesting Subscriber is defined as an Applicant. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request. Prior to verification of identity and issuance of a certificate, any requesting Subscriber is defined as an Applicant.

1.3.3.2 Role of Applicants and/or Subscribers

Before accepting and using a certificate, an Applicant must:

1. Generate a unique Key Pair.
2. Submit an application for the type of certificate requested which must be approved by SSL.com's RA
3. Agree to and accept the terms and conditions of the applicable SSL.com Subscriber Agreement

For Key Pair generation on behalf of the Subscriber, the provisions of §6.2.1 apply.

1.3.3.3 Applicant and/or Subscriber responsibilities

Each Applicant and/or Subscriber is solely responsible for the generation of the Key Pair associated with an SSL.com certificate. For Key Pair generation on behalf of the Subscriber, the provisions of §6.2.1 apply.

Each Applicant and/or Subscriber is solely responsible for the protection of the Private Key related to their SSL.com certificate.

A Subscriber shall immediately notify SSL.com if any information contained in an issued SSL.com certificate changes or becomes false or misleading, or in the event that its Private Key has been compromised or the Subscriber has reason to believe that it has been compromised. A Subscriber must immediately stop using and uninstall any SSL.com certificate upon that certificate's revocation or expiration.

Applicants and Subscribers are required to operate under the SSL.com CP/CPS and agree to the SSL.com Subscriber Agreement.

1.3.4. Relying Parties

A Relying Party is any entity performing transactions, communications and/or functions which rely on a certificate issued by SSL.com.

Before relying on or using an SSL.com certificate, Relying Parties should:

- Read the SSL.com CP/CPS in its entirety
- Review the SSL.com repository to determine whether the certificate has expired or been revoked (per the CRL and/or OCSP) and/or to collect more information concerning the certificate

Relying Parties should make their own judgment as to what degree, if any, they rely on any certificate and must make a trust decision based on the content of the corresponding certificate in order to proceed to specific actions or justified belief. In order to verify the validity of the certificate, Relying Parties must check that:

- The validity period of the certificate has begun and has not expired
- The certificate is correctly signed by an SSL.com Trusted Certification Authority
- The certificate has not been revoked/suspended
- Subject identification matches the details that the signer presents
- The usage for which the certificate was originally intended corresponds with those presented and abides by the terms and the conditions that are described in SSL.com's CP/CPS.

1.3.5 Other participants in the SSL.com PKI

SSL.com shall contractually guarantee that all applicable requirements specified in the CP/CPS, including satisfaction of EV Guidelines, are met in all contracts with Subordinate CAs, external RAs, Enterprise RAs, and/or subcontractors that involve or relate to the issuance or maintenance of Certificates.

For Technically Constrained Subordinate CAs allowed to issue TLS Certificates in line with §7.1.5, SSL.com shall enforce these obligations and internally audit each such entity for compliance with this CP/CPS on an annual basis per §8.7.

For Subordinate CAs that are not Technically Constrained, SSL.com shall require an annual audit performed by a Qualified Auditor per §8.4.

Signing Services MUST support generation of Subscriber Key Pair and maintain security of the Subscriber Private Key.

Timestamp Authorities may be used by the Subscriber to provide timestamp records to indicate data existed at a specific time.

1.4 Certificate usage

1.4.1 Allowed certificate usage

A certificate issued by SSL.com under the guidelines of the SSL.com CP/CPS shall be used only as designated by the key usage or extended key usage fields defined in the certificate profile for

that product (including authentication, encryption, access control, and digital signature purposes).

1.4.2 Prohibited certificate usage

A certificate issued by SSL.com under the guidelines of this SSL.com CP/CPS may not be used for any purpose other than those defined in the certificate profile of the respective product.

Note to Relying Parties: Digitally signed code by a Code Signing Certificate does not guarantee that the code is safe from Suspect Code.

Third parties are not allowed to use TLS Server Certificates issued by SSL.com to conduct surreptitious interception, except with the domain registrant's permission.

1.5 Policy Administration

1.5.1 Organization administering the SSL.com CP/CPS

The SSL.com CP/CPS, related procedural or security policy documents, and any other related agreements referenced, are administered by the SSL.com Policy Management Authority (PMA), appointed by SSL.com management.

1.5.2 Contact information for the SSL.com PMA

The SSL.com PMA can be contacted via the following methods:

- **Mail:**
  - SSL.com
  - 3200 Southwest Fwy Ste 1150
  - Houston, Texas 77027
- **Email:** compliance@ssl.com
- **Phone:** +1 877-775-7328
- **Fax:** +1 832-201-7706

Instructions on how to submit a Certificate Problem Report is provided in §4.9.3.3.

1.5.3 Person determining CP/CPS suitability for the policy

Compliance and suitability with the SSL.com CP/CPS is monitored and managed by the SSL.com PMA, with reference to results and recommendations made by Qualified Auditors and Self-Audits (§8).

1.5.4 CPS approval procedures

The SSL.com CP/CPS is approved and amended by the SSL.com PMA per the provisions of §9.12.

1.6 Definitions and acronyms

1.6.1 Definitions

Account Dashboard: User interface for management of SSL.com Certificates. Any Applicant will be directed to log in to or create an SSL.com account before any request shall be processed.

Address and Routing Parameter Area Name: A Domain Name whose Top-Level Domain is "arpa". Examples: `a.b.c.d.in-addr.arpa` or `....x.x.x.x.ip6.arpa.`.

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of SSL.com or is SSL.com.

Application Software Supplier: A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in §8.1.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of industry standards Requirements.

Authorization Domain Name: The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. SSL.com may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then SSL.com MUST remove `*.` from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. SSL.com may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the

values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

Authorized Port: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. “example.co.uk” or “example.com”). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Business Entity: Any entity that is not a Private Organization, Government Entity, or Non-Commercial Entity as defined herein. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

CAA: For TLS Server Certificates, from RFC 8659: “The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue”. For S/MIME Certificates, from RFC 9495: “The Certification Authority Authorization (CAA) DNS resource record (RR) provides a mechanism for domains to express the allowed set of Certification Authorities that are authorized to issue certificates for the domain.”

CA Key Pair: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

CAB Forum: The Certification Authority/Browser Forum, a voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for TLS and Code Signing. The CAB Forum determines guidelines and requirements to establish public trust in browsers and other software using digital certificates.

CCADB: A repository of information about externally operated Certificate Authorities (CAs) whose root and intermediate certificates are included within the products and services of Application Software Suppliers who are CCADB root store members. The repository is available at https://ccadb.org.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Approver: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV or Mark Certificate Requests submitted by other Certificate Requesters.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which SSL.com verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Management System: A system used by SSL.com or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with §7, e.g. a Section in a CA's CPS or a certificate template file used by CA software.

Certificate Requester: A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV or Mark Certificate Request on behalf of the Applicant.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certificate Systems: The systems used by SSL.com or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Code Signature: A Signature logically associated with a signed Object

Combined Mark: A mark consisting of a graphic design, stylized logo, or image, with words and/or letters having a particular stylized appearance. For greater certainty, a "Combined Mark" includes marks made up of both word and design elements.

Common Mark Certificate: A Mark Certificate that contains a Mark Representation that has not been verified as a Registered Mark or Government Mark.

Confirmation Request: An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue.

Contract Signer: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

Cross-Certified Subordinate CA Certificate: A certificate that is used to establish a trust relationship between two CAs.

CSPRNG: A random number generator intended for use in a cryptographic system.

Dashboard: See Account Dashboard.

Delegated Third Party: A natural person or Legal Entity that is not SSL.com, and whose activities are not within the scope of SSL.com's external audits, but is authorized by SSL.com to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Delegated Third Party System: Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by SSL.com.

Design Mark: A mark consisting of a graphic design, stylized logo, or image, without words and/or letters. For greater certainty, a "Design Mark" includes marks made up solely of design elements.

Designated Individual: The person who completes the F2F Verification Procedure under the provisions of the MC Requirements.

DNS CAA Email Contact: The email address defined as a property in a DNS CAA record. Example: `CAA 0 contactemail "domainowner@example.com"`. The CAA contactemail property takes an email address as its parameter. The entire parameter value MUST be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used. The contactemail property MAY be critical, if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

DNS CAA Phone Contact: The phone number defined as a property in a DNS CAA record. Example: `CAA 0 contactphone "+1 (555) 123-4567"`. The CAA contactphone property takes a phone number as its parameter. The entire parameter value MUST be a valid Global

Number as defined in RFC 3966 section 5.1.4, or it cannot be used. Global Numbers MUST have a preceding + and a country code and MAY contain visual separators. The contactphone property MAY be critical if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

DNS TXT Record Email Contact: The email address placed in a DNS TXT record. The DNS TXT record MUST be placed on the `_validation-contactemail` subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used.

DNS TXT Record Phone Contact: An email address placed in a DNS TXT record. This DNS TXT record MUST be placed on the `_validation-contactphone` subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid Global Number as defined in RFC 3966 section 5.1.4, or it cannot be used.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Label: From RFC 8499: "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

Domain Name: An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Enterprise EV Certificate: An EV Certificate that an Enterprise RA authorizes SSL.com to issue at third and higher domain levels.

Enterprise EV RA: An employee or agent of an organization unaffiliated with SSL.com who authorizes issuance of EV Certificates at third and higher domain levels to that organization.

Enterprise RA: An employee or agent of an organization unaffiliated with SSL.com who authorizes issuance of Certificates to that organization.

EV Certificate: A certificate that contains subject information specified in, and which has been validated in accordance with the EV Guidelines.

EV Certificate Renewal: The process whereby an Applicant who has a valid, unexpired and non-revoked EV Certificate issued by SSL.com, makes an application to SSL.com for a newly issued EV Certificate that includes the same organizational name and Domain Name as the existing EV Certificate, a new 'valid to' date beyond the expiry of the current EV Certificate and the application is prior to the expiration of the Applicant's existing EV Certificate.

EV Certificate Request: A request from an Applicant to SSL.com requesting that SSL.com issue an EV Certificate to the Applicant whose valid request is authorized by the Applicant and signed by the Applicant Representative.

EV Code Signing Certificate: A certificate that contains subject information validated according to the EV Guidelines.

EV OID: An identifying number, in the form of an "object identifier," that is included in the certificatePolicies field of a certificate that: (i) indicates which CA policy statement relates to that certificate, and (ii) by pre-agreement with one or more Application Software Supplier, marks the certificate as being an EV Certificate.

EV Processes: The keys, software, processes, and procedures by which SSL.com verifies Certificate Data, issues EV Certificates, maintains a Repository and revokes EV Certificates.

Expiry Date: The "notAfter" date in a Certificate that defines the end of a Certificate's validity period.

Extant S/MIME CA: A Subordinate CA that:

1. Is a Publicly-Trusted Subordinate CA Certificate whose `notBefore` field is before September 1, 2023 and which is included in a valid trust chain of an end entity S/MIME Certificate;
2. The CA Certificate includes no Extended Key Usage extension, contains `anyExtendedKeyUsage` in the EKU extension, or contains `id-kp-emailProtection` in the EKU extension;
3. The CA Certificate complies with the profile defined in RFC 5280. The following two deviations from the RFC 5280 profile are acceptable: a. The CA Certificate contains a `nameConstraints` extension that is not marked critical; b. The CA Certificate contains a policy qualifier of type UserNotice which contains `explicitText` that uses an encoding that is not permitted by RFC 5280 (i.e., the `DisplayText` is encoded using BMPString or VisibleString); and
4. The CA Certificate contains the `anyPolicy` identifier (2.5.29.32.0) or specific OIDs in the `certificatePolicies` extension that do not include those defined in Section 7.1.6.1 of the S/MIME Baseline Requirements.

Extended Validation Certificate: See EV Certificate.

Fully-Qualified Domain Name: A Domain Name that includes Domain Labels of all superior nodes in the Internet Domain Name System.

F2F Verification Procedure: Either the Notarization process or the web based F2F session as specified in the MC Requirements.

Government Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Government Mark: A Mark or equivalent granted to or claimed by a government organization (or granted to a private organization or other organization) through official statute, regulation, treaty, or government action as it appears or is described in the statute, regulation, treaty, or government action and confirmed by a Mark Verifying Authority using the procedures prescribed in Section §3.2.2.12. A Mark that has been registered by a Government Entity as a trademark with a Trademark Office is not considered a "Government Mark".

Hardware Crypto Module: A tamper-resistant device, with a cryptography processor, used for the specific purpose of protecting the lifecycle of cryptographic keys (generating, managing, processing, and storing).

High Risk Certificate Request: A Request which SSL.com flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names which SSL.com identifies using its own risk-mitigation criteria.

High Risk Region of Concern (HRRC): A geographic location where the detected number of Code Signing Certificates associated with signed Suspect Code exceeds 5% of the total number of detected Code Signing Certificates originating or associated with the same geographic area. This information is provided in Appendix D of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates" document.

Incorporating Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Individual: A natural person.

Individual-Validated: Refers to a Certificate Subject that includes only Individual (Natural Person) attributes, rather than attributes linked to an Organization.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top-Level Domain registered in IANA's Root Zone Database.

Intermediate CA Certificate: A Certificate issued by a Root Certificate or another Intermediate CA Certificate which is deemed as capable of being used to issue new Certificates and which contains an X.509v3 basicConstraints extension, with the cA boolean set to true. If an Intermediate CA Certificate is issued to a non-affiliated organization, then this Intermediate CA Certificate is also referred to as an Intermediate CA Certificate of a Subordinate CA.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top-Level Domain registered in IANA's Root Zone Database.

IP Address: A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

IP Reverse Zone Suffix: One of the two FQDNs that consist of the Domain Labels "in-addr.arpa" or "ip6.arpa". These two FQDNs serve as the root of the IP version 4 and IP version 6 reverse mapping space. "in-addr.arpa" is the root of the IP version 4 reverse mapping space and "ip6.arpa" is the root of the IP version 6 reverse mapping space.

Jurisdiction of Incorporation: In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Jurisdiction of Registration: In the case of a Business Entity, the state, province, or locality where the organization has registered its business presence by means of filings by a Principal Individual involved in the business.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

Key Pair: The Private Key and its associated Public Key.

LDH Label: From RFC 5890: "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."

Latin Notary: A person with legal training whose commission under applicable law not only includes authority to authenticate the execution of a signature on a document but also responsibility for the correctness and content of the document. A Latin Notary is sometimes referred to as a Civil Law Notary.

Legacy Profile: The S/MIME Legacy Generation profiles provide flexibility for existing reasonable S/MIME certificate practices to become auditable under the S/MIME Baseline Requirements. This includes options for Subject DN attributes, extKeyUsage, and other extensions. The Legacy Profiles will be deprecated in a future version of the S/MIME Baseline Requirements.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Legal Existence: A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

Legal Practitioner: A person who is either a lawyer or a Latin Notary (see above) and competent to render an opinion on factual claims of the Applicant.

Lifetime Signing OID: An optional extended key usage OID (`1.3.6.1.4.1.311.10.3.13`) used by Microsoft Authenticode to limit the lifetime of the Code Signature to the expiration of the Code Signing certificate.

Linting: A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a `tbsCertificate` (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in the Baseline Requirements.

Mailbox-Validated (MV): Refers to a Certificate Subject that is limited to (optional) `subject:emailAddress`, `subject:commonName`, and/or `subject:serialNumber` attributes.

Mailbox Address: Also Email Address. The format of a Mailbox Address is defined as a "Mailbox" as specified in Section 4.1.2 of RFC 5321 and amended by Section 3.2 of RFC 6532, with no additional padding or structure.

Mailbox Field: In Subscriber Certificates contains a Mailbox Address of the Subject via `rfc822Name` or `otherName` value of type `id-on-SmtpUTF8Mailbox` in the `subjectAltName` extension, or in Subordinate CA Certificates via `rfc822Name` in permittedSubtrees within the `nameConstraints` extension.

Mark: A Combined Mark, Design Mark, or Word Mark. Such Marks may either be 1. registered with a Trademark Office (Registered Mark) or created through government action (Government Mark); or 2. a mark or logo which qualifies to be included in a Mark Certificate.

Mark Asserting Entity ("MAE"): An Applicant for/Subscriber of a Mark Certificate. May be the same as the Applicant and/or Subscriber.

Mark Certificate: A certificate that contains subject information and extensions specified in these MC Requirements and that has been verified and issued by a MVA in accordance with the MC Requirements.

Mark Representation: A digital representation of a Combined Mark, Design Mark, or Word Mark such as a digital or computer file, containing structured binary or textual data which can be interpreted to recreate (render) a visual representation of the mark so that it can be seen.

Mark Verifying Authority ("MVA"): The authority who issues a Mark Certificate. Also referred to as a Certification Authority or CA.

Multi-Perspective Issuance Corroboration: A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

Multipurpose Profile: The S/MIME Multipurpose Generation profiles are aligned with the more defined Strict Profiles, but with additional options for `extKeyUsage` and other extensions. This is intended to allow flexibility for crossover use cases between document signing and secure email.

Natural Person: An Individual; a human being as distinguished from a Legal Entity.

NAESB: The North American Energy Standards Board.

NAESB Subscribers: Subscribers using SSL.com certificates compliant to NAESB Electric Industry Registry requirements.

Network Perspective: Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

Non-Reserved LDH Label: From RFC 5890: "The set of valid LDH labels that do not have `--` in the third and fourth positions."

Notary: A person whose commission under applicable law includes authority to authenticate the execution of a signature on a document.

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP: See Online Certificate Status Protocol.

OCSP Responder: An online server operated under the authority of SSL.com and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

OID: see Object Identifier.

Onion Domain Name: A Fully Qualified Domain Name ending with the RFC 7686 ".onion" Special-Use Domain Name. For example, `2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion` is an Onion Domain Name, whereas `torproject.org` is not an Onion Domain Name.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate. See also OCSP Responder.

Organization-Validated: Refers to a Certificate Subject that includes only Organizational (Legal Entity) attributes, rather than attributes linked to an Individual.

P-Label: A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.

Parent Company: A company that Controls a Subsidiary Company.

Pending Prohibition: The use of a behavior described with this label is highly discouraged, as it is planned to be deprecated and will likely be designated as MUST NOT in the future.

Personal Name: Personal Name is a name of an Individual Subject typically presented as `subject:givenName` and/or `subject:surname`. However, the Personal Name may be in a format preferred by the Subject, the CA, or Enterprise RA as long as it remains a meaningful representation of the Subject's verified name.

PKI: See Public Key Infrastructure.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant's business is conducted.

Policy Management Authority: Administrative body appointed by SSL.com management to create and maintain policies described in the SSL.com CP/CPA and related procedural or security policy documents.

Primary Network Perspective: The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).

Principal Individual: An individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of EV Certificates.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Pseudonym: A fictitious identity that a person assumes for a particular purpose. Unlike an anonymous identity, a pseudonym can be linked to the person's real identity.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Public Suffix: Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a "public suffix list" such as https://publicsuffix.org/ (PSL), and to retrieve a fresh copy regularly. If using the PSL, a CA SHOULD consult the "ICANN DOMAINS" section only, not the "PRIVATE DOMAINS" section. The PSL is updated regularly to contain new gTLDs delegated by ICANN, which are listed in the "ICANN DOMAINS" section. SSL.com is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of §8.2 (Auditor Qualifications).

Qualified Government Information Source: A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information, provided that it is

1. maintained by a Government Entity,
2. the reporting of data is required by law, and
3. false or misleading reporting is punishable with criminal or civil penalties.

Qualified Government Tax Information Source: A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.

Qualified Independent Information Source: A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

RA: See Registration Authority

Random Value: A value specified by SSL.com to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registered Mark: A Mark that has been registered as a trademark with a Trademark Office, and in particular, as the Mark appears in the official database of the applicable Trademark Office.

Registration Agency: A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency may include, but is not limited to (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Office of the Comptroller of the Currency or Office of Thrift Supervision.

Registration Authority: Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Registration Reference: An identifier assigned to a Legal Entity.

Registration Scheme: A scheme for assigning a Registration Reference meeting the requirements identified in Appendix A of S/MIME Baseline Requirements.

Re-keying: Creation of an entirely new certificate, using some or all of the information submitted for an existing certificate and using a newly generated Private Key.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response. SSL.com maintains its repository at https://www.ssl.com/repository.

Request Token: A value derived in a method specified by SSL.com which binds this demonstration of control to the certificate request.

The Request Token SHALL incorporate the key used in the certificate request.

A Request Token MAY include a timestamp to indicate when it was created.

A Request Token MAY include other information to ensure its uniqueness.

A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.

A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.

A Request Token that does not include a timestamp is valid for a single use and SSL.com SHALL NOT re-use it for a subsequent validation.

The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by SSL.com.

Reserved IP Address: An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries:

- https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
- https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

Root CA: A top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root CA System: A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Root Program Policy: Policy set by an Application Software Supplier to establish the minimum requirements for CA certificates to be distributed in their software.

Signature: An encrypted electronic data file which is attached to or logically associated with other electronic data and which (i) identifies and is uniquely linked to the signatory of the electronic data, (ii) is created using means that the signatory can maintain under its sole control, and (iii) is linked in a way so as to make any subsequent changes that have been made to the electronic data detectable.

Signing Service: An organization that generates the Key Pair and securely manages the Private Key associated with a Code Signing Certificate, on behalf of a Subscriber.

Short-lived Subscriber Certificate: For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).

Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Sponsor-validated: Refers to a Certificate Subject which combines Individual (Natural Person) attributes in conjunction with a `subject:organizationName` (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA where the `subject:organizationName` is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject Organization.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the `subjectAltName` extension or the Subject `commonName` field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use. For Code Signing and EV Code Signing Certificates, the Subscriber is

1. the Subject of the EV Code Signing Certificate and
2. the entity responsible for distributing the software, but does not necessarily hold the copyright to the software.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Subsidiary Company: A company that is controlled by a Parent Company.

Suspect code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, code that compromises user security and/or code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

Takeover Attack: An attack where a Private Key associated with a Code Signing Certificate has been compromised by means of fraud, theft, intentional malicious act of the Subject's agent, or other illegal conduct.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage and/or Name Constraint extensions, as defined within the relevant Certificate Profiles, to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of SSL.com or is SSL.com.

Test Document Signing Certificate: A Document Signing Certificate which includes an extension with the specified Adobe Test Policy Identifier (`1.2.840.113583.1.2.2`), or (ii) is issued under a CA where there are no certificate paths/chains to a root CA certificate subject to any of the requirements of §1.1 of this CP/CPS.

Timestamp Authority: An organization that timestamps data, thereby asserting that the data existed at the specified time.

Top-Level Domain: From RFC 8499: "A Top-Level Domain is a zone that is one layer below the root, such as"com" or "jp"."

Trademark Office: An intellectual property office recognized by the World Intellectual Property Organization for registration of trademarks (see names of intellectual property offices as listed in the column "Office" at https://www.wipo.int/directory/en/urls.jsp.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialist: Someone who performs the information verification duties specified in this CP/CPS.

Validity Period: From RFC 5280, Section 4.1.2.5: "The period of time from notBefore through notAfter, inclusive".

Verified Mark Certificate: A certificate that contains subject information and extensions specified in the MC Requirements and that has been verified and issued by a CA in accordance

with the MC Requirements. Additionally, the certificate contains a Mark Representation that has been verified as a Registered Mark or Government Mark.

Verified Method of Communication: The use of a telephone number, a fax number, an email address, or postal delivery address, confirmed by the CA in accordance with Section 3.2.2.5 of EV Guidelines as a reliable way of communicating with the Applicant.

WebTrust EV Program: The additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities.

WebTrust Program for CAs: The AICPA/CPA Canada WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

WHOIS: information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

Wildcard Certificate: A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.

Wildcard Domain Name: A string starting with `*.` (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

Word Mark: A mark consisting exclusively of text expressed without regard to the font, style, size or color.

XN-Label: From RFC 5890: "The class of labels that begin with the prefix `xn--` (case independent), but otherwise conform to the rules for LDH labels."

1.6.2 Acronyms

Short Term	Explained Term
ADN	Authorization Domain Name
AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CAA	Certification Authority Authorization
CCADB	Common CA Database
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CMC	Common Mark Certificate

Short Term	Explained Term
CP	Certificate Policy
CPA	Chartered Professional Accountant
CP/CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSO	Chief Security Officer
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As
DN	Distinguished Name
EKU	Extended Key Usage
EV	Extended Validation
EVCP	Extended Validation Certificates Policy
FIPS	United States Federal Information Processing Standards
FQDN	Fully-Qualified Domain Name
gTLD	Generic Top-Level Domain
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IM	Instant Messaging
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IV	Individual-Validated
MC	Mark Certificate
NIST	(US Government) National Institute of Standards and Technology
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OV	Organization-Validated
OVCP	Organization Validation Certificates Policy
PIN	Personal identification number

Short Term	Explained Term
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	IETF Working Group on PKI
PMA	Policy Management Authority
QGIS	Qualified Government Information Source
QTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority
SHA	Secure Hashing Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Socket Layer
subCA	Subordinate Certification Authority
SV	Sponsor-Validated
TLD	Top-Level Domain
TLS	Transport Layer Security
URL	Uniform Resource Locator
VMC	Verified Mark Certificate
VoIP	Voice Over Internet Protocol
X.509	ITU-T standard for Certificates and authentication framework

1.6.3 References

The definitions, acronyms and terminology used in the SSL.com CP/CPS may draw from the documents and publications listed below:

Document	Title
FIPS 140-2	Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001
FIPS 140-3	Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, March 22, 2019
FIPS 186-5	Federal Information Processing Standards Publication - Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology, February 2023

Document	Title
ISO 21188:2018	Public key infrastructure for financial services – Practices and policy framework
NIST SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-89.pdf
RFC 822	Standard For the Format of ARPA Internet Text Messages
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels
RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
RFC 3492	Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
RFC 3912	WHOIS Protocol Specification
RFC 3986	Punycode: Uniform Resource Identifier (URI): Generic Syntax
RFC 4035	Protocol Modifications for the DNS Security Extensions
RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
RFC 4509	Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environmentsn
RFC 5155	DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 5702	Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
RFC 5890	Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework
RFC 5952	A Recommendation for IPv6 Address Text Representation
RFC 6454	The Web Origin Concept
RFC 6840	Clarifications and Implementation Notes for DNS Security (DNSSEC)
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
RFC 6962	Certificate Transparency
RFC 7231	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content

Document	Title
RFC 7301	Transport Layer Security (TLS), Application-Layer Protocol Negotiation Extension
RFC 7482	Registration Data Access Protocol (RDAP) Query Format
RFC 7538	The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect)
RFC 8499	DNS Terminology
RFC 8555	Automatic Certificate Management Environment (ACME)
RFC 8659	DNS Certification Authority Authorization (CAA) Resource Record
RFC 8737	Automated Certificate Management Environment (ACME) TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension
RFC 8738	Automated Certificate Management Environment (ACME) IP Identifier Validation Extension
RFC 8823	Extensions to Automatic Certificate Management Environment for End-User S/MIME Certificates
RFC 8954	Online Certificate Status Protocol (OCSP) Nonce Extension
RFC 9336	X.509 Certificate General-Purpose Extended Key Usage (EKU) for Document Signing
RFC 9495	Certification Authority Authorization (CAA) Processing for Email Addresses
RFC 9598	Internationalized Email Addresses in X.509 Certificates
X.509v3	ITU-T Recommendation X.509 (2005) ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

The SSL.com CP/CPS also observes the most current versions of the following documents:

Document	Link
Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates	https://cabforum.org/baseline-requirements-documents/
Guidelines For The Issuance And Management Of Extended Validation Certificates	https://cabforum.org/extended-validation/
Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates	https://cabforum.org/baseline-requirements-code-signing/
Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates	https://cabforum.org/smime-br/

Document	Link
Minimum Security Requirements for Issuance of Mark Certificates	https://bimigroup.org/supporting-documents/
Network and Certificate System Security Requirements	https://cabforum.org/network-security/

1.6.4 Conventions

Terms not otherwise defined in this document shall be defined in applicable agreements, user manuals, Certificate Policies and Certification Practice Statements, of SSL.com.

1.6.4.1 Definitions per RFC 2119

The key words “must”, “must not”, “required”, “shall”, “shall not”, “should”, “should not”, “recommended”, “may”, and “optional” in these documents shall be interpreted in accordance with RFC 2119.

2 SSL.com DOCUMENTS AND REPOSITORY

2.1 Repositories

SSL.com maintains a central Repository to allow access to documents related to SSL.com’s policies and practices, including this CP/CPS, Subscriber and Relying Party agreements and root Certificates. SSL.com’s central Repository is available at https://www.ssl.com/repository.

SSL.com’s central Repository is maintained with resources sufficient to provide a commercially reasonable response time for access at all times. Distributed repositories that include at least the same type of information as the central repository may also exist.

2.2 Publication of certification information

CRL distribution points are included in intermediate and end-entity Certificates. CRLs and OCSP services are publicly available online.

2.2.1 SSL.com PKI CP/CPS

The SSL.com CP/CPS shall always be publicly accessible in the SSL.com Repository.

2.2.2 Certificate Revocation List and On-line Certificate Status Protocol

SSL.com maintains Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responders as public resources which provide Relying Parties with pertinent information regarding the validity or current status of an SSL.com certificate. CRL distribution points are included in intermediate and end-entity Certificates. CRLs and OCSP services are publicly available online.

2.2.2.1 CRLs

CRLs maintained by SSL.com contain lists of serial numbers for all revoked, un-expired Certificates issued by SSL.com. These lists adhere to the standards set out in RFC 5280 for X.509 Certificate Revocation Lists. SSL.com maintains CRLs as described in Sections §4.9.7, §4.9.8 and §4.10 of this CP/CPS.

2.2.2.2 OCSP

OCSP is part of SSL.com's Repository and documents all relevant status information for each certificate issued by SSL.com. This status information is presented by SSL.com's OCSP responding server(s) (also known as the OCSP responder). This resource adheres to the standards set out in RFC 6960. See also Sections §4.9.9, §4.9.10 and §4.10 of this CP/CPS.

2.2.3 SSL.com Certificate Subscriber Agreement

A copy of the latest SSL.com Certificate Subscriber Agreement is available in the SSL.com repository https://www.ssl.com/repository/Subscriber-agreement.

2.2.4 SSL.com Relying Party Agreement and Warranty

A copy of the latest SSL.com Certificate Relying Party Agreement and SSL.com Relying Party Warranty are available in the SSL.com repository at https://www.ssl.com/relying-party-agreement and https://www.ssl.com/relying-party-warranty, respectively.

2.2.5 SSL.com Root and Intermediate Certificates

All Root and Intermediate CA Certificates utilized by the SSL.com PKI are available in the SSL.com Repository listed in §2.1.

2.2.6 Audit Reports

Copies of auditor report letters, including those confirming Extended Validation (EV) certification and other relevant statuses, are available in the SSL.com Repository listed in §2.1.

2.2.7 Additional resources related to SSL.com EV Certificates

The SSL.com Repository contains copies of all documents required by Applicants to request an SSL.com Extended Validation (EV) certificate for SSL or Code Signing usage. These include downloadable .pdf versions of:

- EV Certificate Subscriber Agreement
- Sample EV CPA Letter
- Sample EV Legal Opinion

2.2.8 Disclosure of Verification Sources

The SSL.com Repository contains agency information about the Incorporating Agency or Registration Agency used to validate EV Certificates

This agency information SHALL include at least the following:

- Sufficient information to unambiguously identify the Incorporating Agency or Registration Agency (such as a name, jurisdiction, and website); and,
- The accepted value or values for each of the `subject:jurisdictionLocalityName` (OID: `1.3.6.1.4.1.311.60.2.1.1`), `subject:jurisdictionStateOrProvinceName` (OID: `1.3.6.1.4.1.311.60.2.1.2`), and `subject:jursidictionCountryName` (OID: `1.3.6.1.4.1.311.60.2.1.3`) fields, when a certificate is issued using information from that Incorporating Agency or Registration Agency, indicating the jurisdiction(s) that the Agency is appropriate for; and,
- The acceptable form or syntax of Registration Numbers used by the Incorporating Agency or Registration Agency, if SSL.com restricts such Numbers to an acceptable form or syntax; and,
- A revision history that includes a unique version number and date of publication for any additions, modifications, and/or removals from this list.

2.2.9 Other SSL.com Legal Documents

The SSL.com repository contains copies of the following SSL.com legal documents:

- Terms of Service
- Privacy Policy

2.2.10 Documents not included in the SSL.com Repository

SSL.com does not make publicly available documents or elements of documents deemed as internal, which include security controls, internal security polices, etc. However, these documents are fully disclosed in audits associated with any formal accreditation process that SSL.com adheres to.

2.3. Time or Frequency of Publication

2.3.1 Frequency of Publication of Certificates

Certificate information is published immediately upon acceptance by the Subscriber or when a Certificate is revoked. More information is available in §4.4.2.

2.3.2 Frequency of Publication of CRLs

Frequency of CRL updating and publication is described in §4.9.7

2.3.3 Frequency of Publication of CP/CPS, Terms & Conditions

The SSL.com CP/CPS will be revised and/or amended, and the updated document published, as described in §1.5.4.

2.3.4 Notification of major changes

Major changes to any documents, agreements and resources will be clearly noted in the relevant item when published. SSL.com reserves the right to make minor changes to any item in the Repository if such changes do not substantially affect or modify SSL.com PKI operations, practices and policies. More information is available in §9.12.3.

2.4 Access Controls on Repositories

All online repositories described in §2.2 are publicly and anonymously available on the Internet with read-only access. Only authorized entities within SSL.com have rights to perform modification to documents in these repositories. Restrictions and access-controls are applied to public repositories for protection against enumeration and Denial of Service attacks.

Any participant in the SSL.com PKI (including Applicants, Subscribers and Relying Parties) shall have unlimited read-only access to any item in the SSL.com Repository.

Any participant in the SSL.com PKI accessing the SSL.com Repository and/or other SSL.com directory resources are deemed to have agreed with the provisions of the SSL.com CP/CPS and to any other conditions of usage that SSL.com makes available.

3 NAMING, IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Type of names

All SSL.com Certificates adhere to rules for naming and identification, and (except as specifically detailed in the profile for that certificate type) shall require a Distinguished Name that is in compliance with the ITU X.500 standard for Distinguished Names (DN). Names shall be interpreted using the X.500 and RFC822 standards.

For S/MIME Certificates:

- When the `subject:commonName` of a Certificate issued to an Individual does not contain a Mailbox Address, it is specified as a Personal Name or Pseudonym as described in §7.1.4.2.2(a).
- Names consisting of multiple words are permitted. Given names joined with a hyphen are considered as one single given name. Subjects with more than one given name MAY choose one or several of their given names in any sequence. Subjects MAY choose the order of their given name(s) and surname in accordance with national preference.
- SSL.com MAY allow common variations or abbreviations of Personal Names consistent with local practice.

3.1.2 Need for names to be meaningful, unambiguous and unique

For S/MIME Certificates, Personal Names SHALL be a meaningful representation of the Subject's name as verified in the identifying documentation or Enterprise RA records.

3.1.3 Anonymous, pseudonymous and role-based Certificates

The purpose of a Pseudonym is to provide a unique identifier linked to an Individual in a pseudonymized manner when certain privacy conditions are required. For example, a Pseudonym may be used if a government agency requires officials to sign certain decisions via S/MIME so those decisions trace back to individuals, but emphasize the importance of the role over Individual identity in the Certificate.

SSL.com SHALL NOT allow Certificates to be issued with anonymous or pseudonymous Subscriber information. However, for IDNs, SSL.com MAY include the Punycode version of the IDN as a Subject Name.

SSL.com MAY allow Certificates to include role-based Subscriber information. This information SHALL be verified, validated, and SHALL be submitted along with other verified Subscriber information included in the Subject Identity Information field.

3.1.4 Rules for interpreting various name forms

SSL.com Certificates shall be issued with Distinguished Names interpreted using X.500 standards and ASN.1 syntax.

3.1.5 Uniqueness of names

The full combination of the Subject Attributes (Distinguished name) has to be unique in SSL.com's PKI. Depending on the type of certificate (SSL, S/MIME, Code Signing), different elements/attributes of the certificate ensure uniqueness.

3.1.6 Recognition, authentication, and role of trademarks

Applicants agree by submitting a certificate request to SSL.com that their request does not contain data which in any way interferes with or infringes upon the rights of any third parties in any jurisdiction with respect to trademarks, service marks, trade names, company names, "doing business as" (DBA) names, or any other intellectual property right, and that they are not presenting the data for any unlawful purpose whatsoever. Data covered by this agreement includes but is not limited to any domain name, domain name space, Distinguished Name (DN), or Fully-Qualified Domain Name (FQDN), and/or any trade name or DBA name, contained in any portion of the certificate request.

If the certificate is to include a DBA, a Mark or trade name in any field whatsoever, SSL.com shall verify the Applicant's right to use the DBA, Mark or trade name using the steps detailed in §4.2.

Applicants requesting SSL.com Certificates shall be responsible for the legality of the information they present for verification and/or use in Certificates for any jurisdiction in which such content may be used or viewed.

Any certificate issued using information which is deemed to violate §3.1.6 may be revoked by SSL.com.

Subscribers shall defend, indemnify, and hold SSL.com harmless for any loss or damage resulting from any interference or infringement upon the rights of third parties and shall be responsible for defending all actions against SSL.com.

3.2 Initial identity validation

A valid certificate request SHALL establish possession of the Private Key related to the request.

All requests for Certificates sent to SSL.com SHALL be verified at the level of assurance appropriate to the certificate requested. SSL.com issues different types of digital Certificates (including SSL, Code Signing, personal authentication, Mark and S/MIME Certificates) with varying and appropriate levels of verification including “Extended Validation” (EV).

SSL.com SHALL inspect any document relied upon for verification for alteration or falsification. SSL.com SHALL verify the identity and status of any Applicant as appropriate and required for the certificate requested. Alteration or falsification of any document used in this process, and/or falsification or misrepresentation of the identity or status of any Applicant and/or organization referenced in this process, SHALL constitute grounds for disapproval of a certificate request and/or immediate revocation of any existing certificate relying upon altered or falsified documents or false or misrepresented identity or status.

All information that is supplied by the Applicant SHALL be verified by using an independent source of information or an alternative communication channel before it is included in a Certificate.

For EV Certificates, SSL.com takes all verification steps reasonably necessary to satisfy the EV Verification Requirements set forth in the EV Guidelines.

3.2.1 Method to prove possession of Private Key

Any Applicant for any SSL.com certificate must submit a Certificate Signing Request (CSR). This establishes that the Applicant holds the Private Key corresponding to the Public Key to be included in the requested certificate.

This requirement does not apply when a Key Pair is generated by SSL.com on behalf of a Subscriber (e.g. for Document Signing, Code Signing and EV Code Signing Applicants). In these cases SSL.com shall ensure control of Key Pairs as described in 6.2.1.

3.2.2 Authentication of organization and domain identity

Requests for Certificates which include an organization identity shall be verified using the criteria described below. Items to be verified include the legal existence, legal name, assumed name, legal form, jurisdiction of incorporation or registration of the legal entity, identifier and type of identifier of the legal entity, requested address of the legal entity, and the authority of the requesting party, as applicable. SSL.com shall inspect any document relied upon for these purposes for alteration or falsification.

If the Applicant requests a TLS Certificate that will contain Subject Identity Information comprised only of the countryName field, then SSL.com SHALL verify the country associated with the Subject using a verification process meeting the requirements of §3.2.2.3 of this CP/CPS. If the Applicant requests a TLS Certificate that will contain the countryName field and other Subject Identity Information, then SSL.com SHALL verify the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of §3.2.2.1 of this CP/CPS.

Verification of organization identity in any request for an Extended Validation Certificate shall follow the EV verification procedures described in the EV Guidelines. In particular, before issuing an EV Certificate, SSL.com SHALL ensure that all Subject organization information to be included in the EV Certificate conforms to the requirements of, and is verified in accordance with, EV Guidelines and matches the information confirmed and documented by SSL.com pursuant to its verification processes. Extended validation processes SHALL verify the following:

1. The Applicant's existence and identity, including;
    a. The Applicant's legal existence and identity, as per Section 3.2.2.2 of the EV Guidelines,
    b. The Applicant's physical existence (business presence at a physical address), as per Section 3.2.2.4 of the EV Guidelines,
    c. The Applicant's operational existence (business activity), as per Section 3.2.2.6 of the EV Guidelines, and
    d. The Applicant's assumed name, as per Section 3.2.2.3 of the EV Guidelines (if applicable).
2. That the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Certificate, as per Section 3.2.2.7 of the EV Guidelines;
3. A Verified Method of Communication with the entity to be named as the Subject in the Certificate, as per Section 3.2.2.5 of the EV Guidelines;
4. The Applicant's authorization for the EV Certificate, including;
    a. The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester, as per Section 3.2.2.8 of the EV Guidelines,
    b. That a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use, as per Section 3.2.2.9 of the EV Guidelines; and

c. That a Certificate Approver has signed or otherwise approved the EV Certificate Request, as per Section 3.2.2.10 of the EV Guidelines.

When performing the above, SSL.com MAY take additional verification steps that MAY be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement. Whenever the use of documentation obtained by an Incorporating Agency or Registration Agency is required in this process, SSL.com SHALL only use agencies included in its approved, at time of issuance, List of Approved Incorporating and Registration Agencies. This list is publicly available at https://www.ssl.com/repository (see §2.2.8).

3.2.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, SSL.com shall verify the identity and address of the Applicant. This verification shall use documentation provided by, or through communication with, at least one of the following:

1. A government agency or Incorporating Agency or Registration Agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source as defined in §3.2.2.7;
3. A site visit by SSL.com or a third party who is acting as an agent for SSL.com; or
4. An Attestation Letter, as defined in §1.6.1

SSL.com may use the same documentation or communication described in 1) through 4) above to verify both the Applicant's identity and address.

Alternatively, SSL.com may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that SSL.com determines to be reliable.

3.2.2.2 DBA/Trade Name

If the Subject Identity Information is to include a DBA or trade name, SSL.com shall verify the Applicant's right to use the DBA/trade name with at least one of the following criteria:

1. Documentation provided by, or communication with, government agency or Incorporating Agency or Registration Agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source as defined in §3.2.2.7;
3. Communication with a government agency responsible for the management of such DBAs or trade names;
4. An Attestation Letter accompanied by verifying practitioner credentials; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that SSL.com determines to be reliable.

Use of a DBA or trade name is governed by and further described in §3.1.6.

3.2.2.3 Verification of Country

If the `subject:countryName` field is present, then SSL.com shall verify the country associated with the Subject using one of the following:

1. The IP Address range assignment by country for either
    a. The web site's IP address, as indicated by the DNS record for the web site, or
    b. The Applicant's IP address;
2. The ccTLD of the requested Domain Name;
3. Information provided by the Domain Name Registrar; or
4. A method identified in §3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

This Section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

SSL.com shall confirm that, prior to the date of Certificate issuance, SSL.com has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

SSL.com shall confirm that prior to issuance, SSL.com has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate as follows:

1. When the FQDN is not an Onion Domain Name, SSL.com SHALL validate the FQDN using at least one of the methods listed below; and
2. When the FQDN is an Onion Domain Name, SSL.com SHALL validate the FQDN in accordance with Appendix B of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates" document.

Completed confirmations of Applicant authority may be valid for the issuance of multiple certificates over time. In all cases, the confirmation must have been initiated within the time period specified in the relevant requirement (such as §4.2.1 of this document) prior to certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

Effective March 15th, 2026: DNSSEC validation back to the IANA DNSSEC root trust anchor MUST be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective MUST:

- perform DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
- support NSEC3 as defined in RFC 5155; and
- support SHA-2 as defined in RFC 4509 and RFC 5702; and
- properly handle the security concerns enumerated in RFC 6840 Section 4.

Effective March 15th, 2026: SSL.com MUST NOT use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.

DNSSEC validation back to the IANA DNSSEC root trust anchor MAY be performed on all DNS queries associated with the validation of domain authorization or control by Remote Network Perspectives used for Multi-Perspective Issuance Corroboration.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in §8.7.

SSL.com shall maintain a record of which domain validation method was used to validate each domain, including the relevant Baseline Requirements version number applicable.

Note: FQDNs may be listed in Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method has been retired and MUST NOT be used.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.2.4.3 Phone Contact with Domain Contact

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.2.4.4 Constructed Email to Domain Contact

SSL.com shall confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Note: Once the FQDN has been validated using this method, SSL.com MAY also, at its discretion, issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The Random Value SHALL be unique in each email.

The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Effective March 15, 2028: - SSL.com MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

3.2.2.4.5 Domain Authorization Document

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.2.4.6 Agreed-Upon Change to Website

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.2.4.7 DNS Change

SSL.com shall confirm the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT or CAA record for either

1. an Authorization Domain Name; or
2. an Authorization Domain Name that is prefixed with a Domain Label that begins with an underscore character.

If a Random Value is used, SSL.com SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after

1. 30 days; or
2. if the Applicant submitted the certificate request, the time frame permitted for reuse of validated information relevant to the certificate (such as in §4.2.1 of this CP/CPS or Section 3.2.2.14.3 of the CA/Browser Forum EV Guidelines).

Any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, SSL.com MAY also, at its discretion, issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.8 IP Address

SSL.com shall confirm the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with Section 3.2.2.5.

Any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same IP address as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, SSL.com SHALL NOT also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN, unless SSL.com performs separate validations for each of those other FQDNs using authorized methods. This method is NOT suitable for validating Wildcard Domain Names.

Effective March 15, 2026: - SSL.com MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

3.2.2.4.9 Test Certificate

This method has been retired and MUST NOT be used.

3.2.2.4.10. TLS Using a Random Value

This method has been retired and MUST NOT be used.

3.2.2.4.11 Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

SSL.com does not use this method.

3.2.2.4.13 Email to DNS CAA Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659, Section 3.

Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count

as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, SSL.com MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Effective March 15, 2028: - SSL.com MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

3.2.2.4.14 Email to DNS TXT Contact

SSL.com SHALL confirm the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN.

Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, SSL.com MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Effective March 15, 2028: - SSL.com MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

3.2.2.4.15 Phone Contact with Domain Contact

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

SSL.com SHALL confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response to validate the Authorization Domain Name. Each phone call MAY confirm control of multiple Authorization Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each Authorization Domain Name being verified and they provide a confirming response for each Authorization Domain Name.

This call from SSL.com MUST NOT knowingly be transferred or requested to be transferred, as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, SSL.com may leave the Random Value and the Authorization Domain Name(s) being validated. The Random Value MUST be returned to SSL.com to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, SSL.com MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Effective March 15, 2027: - SSL.com MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

SSL.com SHALL Confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3.

SSL.com MUST NOT be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, SSL.com may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to SSL.com to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, SSL.com MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Effective March 15, 2027: - SSL.com MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

3.2.2.4.18 Agreed-Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

1. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file, and
2. SSL.com MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Value:

1. MUST be located on the Authorization Domain Name, and
2. MUST be located under the "/.well-known/pki-validation" directory, and
3. MUST be retrieved via either the "http" or "https" scheme, and
4. MUST be accessed over an Authorized Port.

If SSL.com follows redirects, the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer.
    a. For validations performed on or after July 1, 2021, redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
    b. For validations performed prior to July 1, 2021, redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.
2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.
3. Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

1. SSL.com MUST provide a Random Value unique to the certificate request.
2. The Random Value MUST remain valid for use in a confirming response for no more than 30 days from its creation.

Except for Onion Domain Names, any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

Note: SSL.com MUST NOT issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN unless it performs separate validations for each of those other FQDNs using authorized methods. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555. The following are additive requirements to RFC 8555.

SSL.com MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The token (as defined in RFC 8555, section 8.3) MUST NOT be used for more than 30 days from its creation.

If SSL.com follows redirects, the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer.
    a. For validations performed on or after July 1, 2021, redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
    b. For validations performed prior to July 1, 2021, redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.
2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.
3. Redirects MUST be to resource URLs accessed via Authorized Ports.

Except for Onion Domain Names, any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. token) as the Primary Network Perspective.

Note: SSL.com MUST NOT issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN unless it performs separate validations for each of those other FQDNs using authorized methods. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.20 TLS Using ALPN

SSL.com shall confirm the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application-Layer Protocol Negotiation (ALPN) Extension RFC 7301 as defined in RFC 8737. The following are additive requirements to RFC 8737.

The token (as defined in RFC 8737, Section 3) MUST NOT be used for more than 30 days from its creation.

Except for Onion Domain Names, any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. token) as the Primary Network Perspective.

Note: SSL.com MUST NOT issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN unless it performs separate validations for each of those other FQDNs using authorized methods. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.21 DNS Labeled with Account ID - ACME

Confirming the Applicant's control over the FQDN by performing the procedure documented for a "dns-account-01" challenge in draft 00 of "Automated Certificate Management Environment (ACME) DNS Labeled With ACME Account ID Challenge," available at https://datatracker.ietf.org/doc/draft-ietf-acme-dns-account-label/.

The token (as defined in draft 00 of "Automated Certificate Management Environment (ACME) DNS Labeled With ACME Account ID Challenge," Section 3.1) MUST NOT be used for more than 30 days from its creation.

When performing validations using this method, SSL.com MUST implement Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same token as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, SSL.com MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.5 Authentication for an IP Address

SSL.com SHALL confirm that prior to issuance, SSL.com has validated the Applicant's ownership or control of each IP Address listed in a Certificate using at least one of the methods specified in this section.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in §4.2.1 prior to Certificate issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

After July 31, 2019, SSL.com SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address.

Note: IP Addresses verified in accordance with this §3.2.2.5 may be listed in Subscriber Certificates as defined in §7.1.4.2 or in Subordinate CA Certificates via iPAddress in permittedSubtrees within the Name Constraints extension. SSL.com is not required to verify IP Addresses listed in Subordinate CA Certificates via iPAddress in excludedSubtrees in the Name Constraints extension prior to inclusion in the Subordinate CA Certificate.

3.2.2.5.1 Agreed-Upon Change to Website

SSL.com SHALL confirm the Applicant's control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by SSL.com via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, SSL.com SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the certificate request, the time frame permitted for reuse of validated information relevant to the certificate (see §4.2.1).

Any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

SSL.com SHALL confirm the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as an IP Address Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple IP Addresses.

SSL.com MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail.

SSL.com MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Effective March 15, 2027: - SSL.com MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

3.2.2.5.3 Reverse Address Lookup

SSL.com SHALL confirm the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under §3.2.2.4.

Any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same FQDN as the Primary Network Perspective.

3.2.2.5.4 Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.5.5 Phone Contact with IP Address Contact

SSL.com SHALL confirm the Applicant's control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the Applicant's request for validation of the IP Address. SSL.com MUST place the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact. Each phone call SHALL be made to a single number.

In the event that someone other than an IP Address Contact is reached, SSL.com MAY request to be transferred to the IP Address Contact.

In the event of reaching voicemail, SSL.com may leave the Random Value and the IP Address(es) being validated. The Random Value MUST be returned to SSL.com to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Effective March 15, 2027: - SSL.com MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

3.2.2.5.6 ACME “http-01” method for IP Addresses

SSL.com SHALL confirm the Applicant’s control over the IP Address by performing the procedure documented for an “http-01” challenge in RFC 8738.

Any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. token) as the Primary Network Perspective.

3.2.2.5.7 ACME “tls-alpn-01” method for IP Addresses

SSL.com SHALL confirm the Applicant’s control over the IP Address by performing the procedure documented for a “tls-alpn-01” challenge in RFC 8738.

Any domain validations and CAA checks performed on or after 2025-03-15 using this method SHALL be based on Multi-Perspective Issuance Corroboration as specified in §3.2.2.13. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. token) as the Primary Network Perspective.

3.2.2.6 Wildcard Domain Validation

SSL.com shall follow specific practices to validate any certificate containing a wildcard character (*).

Before issuing a Wildcard Certificate, SSL.com shall determine if the FQDN portion of any Wildcard Domain Name in the Certificate is “registry-controlled” or is a “public suffix” (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation).

If the FQDN portion of any Wildcard Domain Name is “registry-controlled” or is a “public suffix”, SSL.com SHALL NOT issue a Certificate unless the Applicant proves its rightful control of the entire Domain Namespace. (e.g. SSL.com SHALL NOT issue “*.co.uk” or “*.local”, but MAY issue “*.example.com” to Example Co.).

In all such cases, SSL.com shall observe stipulations and considerations as given in RFC 6454 Section 8.2.

Determination of what is “registry-controlled” versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. SSL.com follows the current best practice and consults the Public Suffix List (PSL), and regularly retrieves a fresh copy.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, SSL.com shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

Criteria for this evaluation shall include:

- 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.

For S/MIME Certificates, Enterprise RA records are a Reliable Data Source for Individual Subject attributes included in Sponsor-validated Certificates issued to the Enterprise RA's Organization.

Prior to using any data source as a QIIS, SSL.com SHALL:

1. Ensure that:
    a. Industries other than the certificate industry rely on the database for accurate location, contact, or other information; and
    b. The database provider updates its data on at least an annual basis.
2. Check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider's terms of use. In particular, SSL.com SHALL NOT use any data in a QIIS that SSL.com knows is
    a. self-reported and
    b. not verified by the QIIS as accurate.

3.2.2.8 CAA Records

As part of the TLS or Mark Certificate issuance process, SSL.com MUST retrieve and process CAA records in accordance with RFC 8659 for each `dNSName` in the `subjectAltName` extension that does not contain an Onion Domain Name. These practices are described in §4.2, including specifying the set of Issuer Domain Names that SSL.com recognizes in CAA "issue" or "issuewild" records as permitting it to issue.

Some methods relied upon for validating the Applicant's ownership or control of the subject domain(s) (see §3.2.2.4) or IP address(es) (see §3.2.2.5) to be listed in a certificate require CAA records to be retrieved and processed from additional remote Network Perspectives before Certificate issuance (see §3.2.2.13). To corroborate the Primary Network Perspective, a remote Network Perspective's CAA check response MUST be interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. Additionally, SSL.com MAY consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in this section.

SSL.com MAY check CAA records at any other time.

When processing CAA records for the issuance of TLS Certificates, SSL.com must process the `issue`, `issuewild`, and `iodef` property tags as specified in RFC 8659, although SSL.com is not required to act on the contents of the `iodef` property tag. Additional property tags MAY be supported, but MUST NOT conflict with or supersede the mandatory property tags set out in the Baseline Requirements. Additional property tags may be supported, but must not conflict with or supersede the mandatory property tags set out in this document. SSL.com must respect the critical flag and not issue a certificate if an unrecognized property with this flag set is encountered.

When processing CAA records for the issuance of Mark Certificates, SSL.com must process the `issuevmc` property tag as specified in RFC 8659. CAA records with `issue` or `issuewild` Property Tags do not restrict the issuance of Mark Certificates. The sub-syntax of the `issuevmc` Property Tag value is treated the same as the `issue` Property Tag as defined in section 4.2 of RFC 8659. The semantics of the `issuevmc` Property Tag are similar to the `issue` Property Tag, with the only difference being that the `issuevmc` Property Tag restricts issuance of Mark Certificates as opposed to TLS Server Authentication Certificates.

If SSL.com issues a TLS certificate after processing a CAA record, it MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

RFC 8659 requires that a CA "MUST NOT issue a certificate unless the CA determines that either (1) the certificate request is consistent with the applicable CAA RRset or (2) an exception specified in the relevant CP or CPS applies." For issuances conforming to this CP/CPS, SSL.com must not rely on any exceptions specified in this CP/CPS unless they are one of the following:

1. CAA checking is optional for certificates for which a Certificate Transparency Precertificate (see Section 7.1.2.9 for Precertificate Profile) was created and logged in at least two public logs, and for which CAA was checked at time of Precertificate issuance.
2. CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements Section 7.1.2.3 or 7.1.2.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.

SSL.com is permitted to treat a record lookup failure as permission to issue if:

1. the failure is outside SSL.com's infrastructure;
2. the lookup has been retried at least once; and
3. SSL.com has confirmed that the domain is "Insecure" as defined in RFC 4035 Section 4.3.

SSL.com MUST document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/Browser Forum on the circumstances, and SHOULD dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. SSL.com is not expected to support URL schemes in the iodef record other than mailto: or https:.

3.2.2.8.1 DNSSEC Validation of CAA Records

Effective March 15th, 2026: DNSSEC validation back to the IANA DNSSEC root trust anchor MUST be performed on all DNS queries associated with CAA record lookups performed by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with CAA record lookups performed by the Primary Network Perspective MUST:

- perform DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
- support NSEC3 as defined in RFC 5155; and
- support SHA-2 as defined in RFC 4509 and RFC 5702; and
- properly handle the security concerns enumerated in RFC 6840 Section 4.

Effective March 15th, 2026: SSL.com MUST NOT use local policy to disable DNSSEC validation on any DNS query associated CAA record lookups.

Effective March 15th, 2026: DNSSEC-validation errors observed by the Primary Network Perspective (e.g., SERVFAIL) MUST NOT be treated as permission to issue.

DNSSEC validation back to the IANA DNSSEC root trust anchor MAY be performed on all DNS queries associated with CAA record lookups performed by Remote Network Perspectives as part of Multi-Perspective Issuance Corroboration.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in Section 8.7.

3.2.2.9 Validation of mailbox authorization or control

This section defines the permitted processes and procedures for confirming the Applicant's control of Mailbox Addresses to be included in issued Certificates.

SSL.com SHALL verify that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate or has been authorized by the email account holder to act on the

SSL.com SHALL NOT delegate the verification of mailbox authorization or control.

Completed validations of Applicant authority MAY be valid for the issuance of multiple Certificates over time. In all cases, the validation SHALL have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1) prior to Certificate issuance.

3.2.2.9.1 Validating authority over mailbox via domain

SSL.com MAY confirm the Applicant, such as an Enterprise RA, has been authorized by the email account holder to act on the account holder's behalf by verifying the entity's control over the domain portion of the Mailbox Address to be used in the Certificate.

An Applicant that confirms control of the domain part of an email address is authorized for any local part followed by the at-sign ("@"), followed by the Authorization Domain Name or by any

other Domain Name that ends with all the Domain Labels of the validated Authorization Domain Name.

SSL.com SHALL use only the approved methods described in §3.2.2.4 to perform this verification.

For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

3.2.2.9.2 Validating control over mailbox via email

SSL.com MAY confirm the Applicant's control over each Mailbox Field to be included in a Certificate by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

Control over each Mailbox Address SHALL be confirmed using a unique Random Value. The Random Value SHALL be sent only to the email address being validated and SHALL not be shared in any other way.

The Random Value SHALL be unique in each email. The Random Value SHALL remain valid for use in a confirming response for no more than 24 hours from its creation.

The Random Value SHALL be reset upon each instance of the email sent by SSL.com to a Mailbox Address, however all relevant Random Values sent to that Mailbox Address MAY remain valid for use in a confirming response within the validity period described in this Section.

In addition, the Random Value SHALL be reset upon first use by the user if intended for additional use as an authentication factor following the Mailbox Address verification.

3.2.2.9.3 Validating applicant as operator of associated mail server(s)

SSL.com MAY confirm the Applicant's control over each Mailbox Field to be included in the Certificate by confirming control of the SMTP FQDN to which a message delivered to the Mailbox Address should be directed. The SMTP FQDN SHALL be identified using the address resolution algorithm defined in RFC 5321 Section 5.1 which determines which SMTP FQDNs are authoritative for a given Mailbox Address. If more than one SMTP FQDN has been discovered, SSL.com SHALL verify control of an SMTP FQDN following the selection process at RFC 5321 Section 5.1. Aliases in MX record RDATA SHALL NOT be used for this validation method.

To confirm the Applicant's control of the SMTP FQDN, SSL.com SHALL use only the currently-approved methods described in §3.2.2.4.

3.2.2.9.4 Validating control over mailbox using ACME extensions

SSL.com MAY confirm the Applicant's control over each Mailbox Field to be included in a Certificate using ACME for S/MIME as defined in RFC 8823. SSL.com's ACME server MAY respond to a POST request by sending the Random Value token components via email and

SMTP, and then receiving a confirming response utilizing the generated Random Value, in accordance with RFC 8823.

Control over each Mailbox Address SHALL be confirmed using a newly-generated Random Value. The Random Value token components SHALL only be shared in accordance with RFC 8823. As defined by RFC 8823, `token-part1` SHALL contain at least 128 bits of entropy and `token-part2` SHOULD contain at least 128 bits of entropy.

The Random Value SHALL NOT be reused by SSL.com for other Certificate Requests. The Random Value SHALL remain valid for use in a confirming response for no more than 24 hours from its creation.

Implementations MAY use ACME External Account Binding as defined by RFC 8555.

3.2.2.10 Mark Verification in Verified Mark Certificates

SSL.com issues Verified Mark Certificates (VMCs) for Marks registered with a Trademark Office and qualify as a Registered Mark. These Marks can be Combined Marks, Design Marks, or Word Marks.

3.2.2.10.1 Verification of Mark with Trademark Office

SSL.com SHALL verify the:

1. Registered Mark's trademark registration number and name of the Trademark Office that granted the trademark registration; and
2. Mark Representation in SVG format that the Applicant wishes to include in the Verified Mark Certificate. Registered Marks MUST be in good standing and MUST be verified through consultation with the official database of the applicable Trademark Office.

As an alternative, the Validation Specialist MAY verify the Registered Mark through the WIPO Global Brand Database at https://www.wipo.int/reference/en/branddb/.

3.2.2.10.2 Verification of Registered Mark Ownership or License

SSL.com SHALL confirm that the owner of the Registered Mark identified in the official database of the applicable Trademark Office or the WIPO Global Brand Database is the same Subject organization verified in §3.2.2.1.

3.2.2.10.3 Confirmation of Mark Representation

SSL.com SHALL verify that the Mark submitted by the Applicant exactly matches the Registered Mark on record. This verification will be documented by comparing the Mark with the official database of the relevant Trademark Office or the WIPO Global Brand Database.

3.2.2.10.4 Color Restrictions

Verified Mark Certificates for Combined and Design Marks can only display colors explicitly permitted for the Registered Mark by the relevant trademark office, if any. SSL.com SHALL

review the registration to identify any specific colors claimed by the owner of the registered mark.

3.2.2.11 Mark Verification in Common Mark Certificates

SSL.com issues Common Mark Certificates (MCs) for a Mark Representation that has not been verified as a Registered Mark or Government Mark.

3.2.2.11.1 Verification of Prior Use of Mark for Minimum Period

This type of Mark Certificate is appropriate for Common Marks that are not Registered Marks.

The Applicant will provide SSL.com with the Mark Representation in SVG format that the Applicant wishes to include in the Mark Certificate. SSL.com SHALL verify that:

1. a Mark that matches the Mark Representation is currently displayed on a website. The Applicant's control of the Domain Name of the website MUST be verified using at least one method specified in Section 3.2.14 of the MC Guidelines, and
2. a Mark that matches the Mark Representation was historically displayed at least 12 months earlier than the date of Mark verification on the same Domain Name that was verified as being controlled by the Applicant in (1). The historical display MUST be verified via one of the Archive Webpage Sources allowed by these Requirements.

SSL.com SHALL also retain a screenshot or other record of the Mark Representation provided by the Applicant and all Mark images found during the verification process stated in the previous paragraph.

3.2.2.11.2 Approved Archive Webpage Sources

Validations of Mark Representations performed in accordance with §3.2.2.11.1 SHALL employ one of the following Archive Webpage Sources:

- archive.org

This approved list may be modified from time to time.

3.2.2.11.3 Color Restrictions

Mark Representations in Mark Certificates based on proof of prior use shall follow the same color rules that apply to Common Marks in the applicable jurisdiction. SSL.com SHALL review the prior use to identify any specific colors claimed by the owner of the Mark Representation.

3.2.2.12 Government Mark Verification

SSL.com issues Government Mark Certificates for a Mark or equivalent granted to or claimed by a Government Entity or Non-Commercial Entity (International Organization) (or granted to a private organization or other organization by a Government Entity or Non-Commercial Entity [International Organization] through official statute, regulation, treaty, or government action)

as it appears or is described in the statute, regulation, treaty, or government action and confirmed by a Mark Verifying Authority.

3.2.2.12.1 Verification of Statute, Regulation, Treaty, or Action

SSL.com MUST confirm that the Government Mark has been granted to, or claimed by, a Government Entity or a Non-Commercial Entity (International Organization) by verifying the grant or claim in publicly available records of the applicable statute, regulation, treaty, or government action.

SSL.com MUST retain a copy of the statute, regulation, treaty, or government action, including all official references (e.g., statute or regulation number and jurisdiction), as well as a copy of the Mark as contained in or referenced by the statute or regulation.

A Government Mark may also be granted to private or other types of organizations by Government or Non-Commercial Entities through an official statute, regulation, treaty, or government action.

3.2.2.12.2 Verification of Government Mark Ownership or License

SSL.com MUST confirm that the owner of the Government Mark identified in Section §3.2.2.12.1 either: 1. is the same Subject Organization (Applicant) verified through the Verified Mark Identity vetting process; or 2. has granted the Subject Organization (Applicant) the right to use the Government Mark pursuant to applicable statute, regulation, treaty, or government action, or through a mutually agreed-upon license.

If the owner of record of the Government Mark is not the Applicant, the Applicant MAY use the Government Mark only if SSL.com obtains a written authorization letter from the owner of record of the Government Mark.

3.2.2.12.3 Confirmation of Mark Representation

SSL.com SHALL confirm that the Mark Representation submitted by the Applicant matches the Government Mark as confirmed under Section §3.2.2.12.1.

3.2.2.12.4 Color Restrictions

SSL.com MUST review the Government Mark submitted for inclusion in a Government Mark Certificate and ensure that only the colors permitted, if any, under the applicable statute, regulation, treaty, or government action are used.

3.2.2.13 Multi-Perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance. This process can improve protection against equally-specific prefix Border Gateway Protocol (BGP) attacks or hijacks.

SSL.com MAY use either the same set, or different sets of Network Perspectives when performing Multi-Perspective Issuance Corroboration for the required 1) Domain Authorization or Control and 2) CAA Record checks.

The set of responses from the relied upon Network Perspectives MUST provide SSL.com with the necessary information to allow it to affirmatively assess:

a. the presence of the expected 1) Random Value, 2) Request Token, 3) IP Address, or 4) Contact Address, as required by the relied upon validation method specified in Sections §3.2.2.4 and §3.2.2.5; and
b. the CA's authority to issue to the requested domain(s), as specified in §3.2.2.8.

§3.2.2.4 and §3.2.2.5 describe the validation methods that require the use of Multi-Perspective Issuance Corroboration and how a Network Perspective can corroborate the outcomes determined by the Primary Network Perspective.

Results or information obtained from one Network Perspective MUST NOT be reused or cached when performing validation through subsequent Network Perspectives (e.g., different Network Perspectives cannot rely on a shared DNS cache to prevent an adversary with control of traffic from one Network Perspective from poisoning the DNS cache used by other Network Perspectives). The network infrastructure providing Internet connectivity to a Network Perspective MAY be administered by the same organization providing the computational services required to operate the Network Perspective. All communications between a remote Network Perspective and the CA MUST take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

A Network Perspective MAY use a recursive DNS resolver that is NOT co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective MUST fall within the same Regional Internet Registry service region as the Network Perspective relying upon it. Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two DNS resolvers MUST be at least 500 km. The location of a DNS resolver is determined by the point where unencapsulated outbound DNS queries are typically first handed off to the network infrastructure providing Internet connectivity to that DNS resolver.

SSL.com MAY immediately retry Multi-Perspective Issuance Corroboration using the same validation method or an alternative method (e.g., a CA can immediately retry validation using "Email to DNS TXT Contact" if "Agreed-Upon Change to Website - ACME" does not corroborate the outcome of Multi-Perspective Issuance Corroboration). When retrying Multi-Perspective Issuance Corroboration, SSL.com MUST NOT rely on corroborations from previous attempts. There is no stipulation regarding the maximum number of validation attempts that may be performed in any period of time.

The "Quorum Requirements" Table describes quorum requirements related to Multi-Perspective Issuance Corroboration. If SSL.com does NOT rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum

requirements MUST be met for both sets of Network Perspectives (i.e.,the Domain Authorization or Control set and the CAA record check set). Network Perspectives are considered distinct when the straight-line distance between them is at least 500 km. Network Perspectives are considered "remote" when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

SSL.com MAY reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives MAY omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days.

Quorum Requirements

# of Distinct Remote Network Perspectives Used	# of Allowed non-Corroborations
2-5	1
6+	2

Remote Network Perspectives performing Multi-Perspective Issuance Corroboration:

MUST:

- Network Hardening
    - Rely upon networks (e.g., Internet Service Providers or Cloud Provider Networks) implementing measures to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the Network Perspective.

SHOULD:

- Facility & Service Provider Requirements
    - Be hosted from an ISO/IEC 27001 certified facility or equivalent security framework independently audited and certified or reported.
    - Rely on services covered in one of the following reports: System and Organization Controls 2 (SOC 2), IASE 3000, ENISA 715, FedRAMP Moderate, C5:2020, CSA STAR CCM, or equivalent services framework independently audited and certified or reported.
- Vulnerability Detection and Patch Management
    - Implement intrusion detection and prevention controls to protect against common network and system threats.
    - Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.
    - Undergo or perform a Vulnerability Scan at least every three (3) months.
    - Undergo a Penetration Test on at least an annual basis.
    - Apply recommended security patches within six (6) months of the security patch's availability, unless the CA documents that the security patch would

introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

- System Hardening
  - Disable all accounts, applications, services, protocols, and ports that are not used.
  - Implement multi-factor authentication for all user accounts.
- Network Hardening
  - Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications identified as necessary to its operations.
  - Rely upon networks (e.g., Internet Service Providers) that: 1) use mechanisms based on Secure Inter-Domain Routing (RFC 6480), for example, BGP Prefix Origin Validation (RFC 6811), 2) make use of other non-RPKI route-leak prevention mechanisms (such as RFC 9234), and 3) apply current best practices described in BCP 194. While It is RECOMMENDED that under normal operating conditions Network Perspectives performing Multi-Perspective Issuance Corroboration forward all Internet traffic via a network or set of networks that filter RPKI-invalid BGP routes as defined by RFC 6811, it is NOT REQUIRED.

Beyond the above considerations, computing systems performing Multi-Perspective Issuance Corroboration are considered outside of the audit scope described in §8 of these Requirements.

If any of the above considerations are performed by a Delegated Third Party, SSL.com MAY obtain reasonable evidence from the Delegated Third Party to ascertain assurance that one or more of the above considerations are followed. As an exception to §1.3.2, Delegated Third Parties are not required to be within the audit scope described in §8 of these Requirements to satisfy the above considerations.

Phased Implementation Timeline:

- *Effective September 15, 2024*, SSL.com SHOULD implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives.
- *Effective March 15, 2025*, SSL.com MUST implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. SSL.com MAY proceed with certificate issuance if the number of remote Network Perspectives that do not corroborate the determinations made by the Primary Network Perspective ("non-corroborations") is greater than allowed in the Quorum Requirements table.

- *Effective September 15, 2025*, SSL.com MUST implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. SSL.com MUST ensure that the requirements defined in Quorum Requirements Table are satisfied. If the requirements are not satisfied, then SSL.com MUST NOT proceed with issuance of the Certificate.

- *Effective March 15, 2026*, SSL.com MUST implement Multi-Perspective Issuance Corroboration using at least three (3) remote Network Perspectives. SSL.com MUST ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then SSL.com MUST NOT proceed with issuance of the Certificate.

- *Effective June 15, 2026*, SSL.com MUST implement Multi-Perspective Issuance Corroboration using at least four (4) remote Network Perspectives. SSL.com MUST ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then SSL.com MUST NOT proceed with issuance of the Certificate.
- *Effective December 15, 2026*, SSL.com MUST implement Multi-Perspective Issuance Corroboration using at least five (5) remote Network Perspectives. SSL.com MUST ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then SSL.com MUST NOT proceed with issuance of the Certificate.

3.2.3 Authentication of individual identity

3.2.3.1 Natural Person as an individual Applicant

If an Applicant is a natural person applying as an individual, then SSL.com shall verify the Applicant's name and the authenticity of the certificate request.

For Server Authentication certificates, Code Signing certificates, or when the Applicant's address is displayed in the SubjectDN of the certificate, SSL.com shall also verify the Applicant's address.

For server certificates, SSL.com SHALL verify:

- the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). SSL.com SHALL inspect the copy for any indication of alteration or falsification.
- the Applicant's address using a form of identification that the CA determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. SSL.com MAY rely on the same government-issued ID that was used to verify the Applicant's name.
- the certificate request with the Applicant using a Reliable Method of Communication.

For Code Signing certificates, verification shall be through one or more of the methods described in the Minimum Requirements for Code Signing.

For Extended Validation Certificates, SSL.com shall follow the EV verification procedures as described in the EV Guidelines. Verification for EV Code Signing certificates must meet requirements in both the Minimum Requirements for Code Signing and the EV Guidelines.

For Document Signing Certificates, SSL.com shall rely on strong identity proofing, based on a face to face meeting with the Applicant, or a procedure that provides an equivalent assurance. The latter may include any of the following:

- means of secure video communication;
- use of identity verification software/AI;
- hybrid or other methods.

For S/MIME Certificates, the following requirements SHALL be fulfilled to authenticate Individual identity attributes included in `Sponsor-validated` and `Individual-validated` Certificate profiles:

1. SSL.com, the RA, or the Enterprise RA SHALL collect and retain evidence supporting the following identity attributes for the Individual Applicant:
    a. Given name(s) and surname(s), which SHALL be current names;
    b. Title (if used);
    c. Address (if displayed in Subject); and
    d. Further information as needed to uniquely identify the Applicant.
2. SSL.com or the RA SHALL comply with applicable data protection legislation in the gathering and retention of evidence relating to Individual identity supporting this Requirement in accordance with Section 9.4.
3. The above-mentioned identity proofing methods utilized for Document Signing Certificates MAY also be used for S/MIME Certificates.

3.2.3.2 Natural Person associated with a Legal Entity

For Document Signing, S/MIME and Client Authentication Certificates issued to Natural Persons associated with Legal Entities, SSL.com

- shall validate the Legal Entity following the requirements of §3.2.2.1;
- shall obtain evidence that the individual is associated with the Legal Entity.

For Document Signing Certificates, SSL.com shall perform identity verification of individual natural persons associated with that Legal Entity following the requirements of §3.2.3.1.

For S/MIME and Client Authentication Certificates, SSL.com may also rely on the Legal Entity to perform identity verification of individual natural persons associated with that Legal Entity.

For S/MIME Certificates, an Enterprise RA issuing a Sponsor-validated Certificate SHALL validate all identity attributes of an Individual to be included in the Certificate. The Enterprise RA MAY rely upon existing internal records to validate Individual identity.

3.2.4 Non-verified information

SSL.com does not verify information contained in the Organization Unit (OU) field in any certificate request, and only ensures that the OU attribute meets the requirements described in §7.1.4.2.2 i. Other information may be designated as non-verified in specific certificate profiles. Non-verified information other than the OU field will be detailed in the certificate profile and in the verification process for that certificate type as given in §4.

SSL.com may waive its standard identity validation procedures for Test Document Signing Certificates. Any such certificates SHALL clearly indicate that they are for testing purposes, as specified in §7.1.6.

3.2.5 Validation of authority

SSL.com shall verify the authorization of all certificate requests.

For server certificate requests:

- If the Applicant for a Certificate containing Subject Identity Information is an organization, SSL.com SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.
- SSL.com MAY use the sources listed in §3.2.2.1 to verify the Reliable Method of Communication. Provided that a Reliable Method of Communication is used, SSL.com MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that SSL.com deems appropriate.
- In addition, SSL.com SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then SSL.com SHALL NOT accept any certificate requests that are outside this specification. SSL.com SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

For Code Signing certificate requests, verification of this authority shall be through one or more of the methods described in the Code Signing Baseline Requirements. Verification of authority for EV Code Signing certificates must meet the EV requirements described in the Code Signing Baseline Requirements.

For Extended Validation TLS Certificate requests, SSL.com shall follow procedures described in the EV Guidelines to verify the authority of the request.

3.2.6 Criteria for interoperation

SSL.com MAY issue Cross-Certified Subordinate CA Certificates as required in order to assist root roll-over operations.

SSL.com MAY issue Cross-Certified Subordinate CA Certificates to other CA operators provided there is alignment with this CP/CPS and SSL.com arranged for or accepted the establishment of the trust relationship (i.e. the Cross-Certified Subordinate CA Certificate at issue). The cross certification terms and criteria are to be set forth in an applicable agreement.

All Cross-Certified Subordinate CA Certificates that identify SSL.com as the Subject SHALL be disclosed in CCADB and the SSL.com Repository.

3.3 Identification and authentication for re-keying

Re-keying (sometimes called reissuing) refers to the issuance of an entirely new certificate, using some or all of the information submitted for an existing certificate and using a newly generated Private Key.

Subscribers may request re-keying of an SSL.com certificate prior to the certificate's expiration.

Subordinate CAs of SSL.com may request re-keying of a certificate registered by them prior to the certificate's expiration. The re-keying process is detailed fully in §4.7.

This section is not applicable to Mark Certificates.

3.3.1 Re-keying request by Subscriber

3.3.1.1 Subscriber re-keying request via SSL.com Account Dashboard

A Subscriber may request re-key of any unexpired SSL.com certificate via their SSL.com Account Dashboard. Any changes made when requesting re-keying by this method may require validation and/or authentication steps as described in §4.7.

3.3.1.2 Subscriber re-keying request via other means

A Subscriber requesting re-keying of an unexpired SSL.com certificate by any method other than their SSL.com Account Dashboard requires validation and/or authentication steps as described in §4.7.

3.3.2 Identification and authentication for re-key after revocation

A Subscriber requesting re-key of an SSL.com certificate after that certificate has been revoked will need to apply for and follow all validation and/or authentication procedures for a new certificate.

3.4 Identification and authentication for revocation requests

SSL.com may revoke any certificate issued within the SSL.com PKI at its sole discretion. In all cases, identification and/or authorization for a revocation request must follow the procedures detailed in §4.9.3.

3.4.1 Identification and authentication for revocation requests by Subscribers

A Subscriber, or the Subscriber's authorized agent, may request revocation of any unexpired SSL.com certificate via their SSL.com Account Dashboard.

Revocation requests from a Subscriber or authorized agent for an unexpired SSL.com certificate by any method other than their SSL.com Account Dashboard may, at SSL.com's sole discretion, require further validation and/or authentication steps as described in §4.9.

SSL.com may, if necessary, and at its sole discretion, confirm a revocation request by other means, including (but not limited to) contact with the Subscriber or authorized representatives of the Subscriber.

3.4.2 Revocation requests by non-Subscribers

Non-Subscribers (such as Relying Parties, Application Software Suppliers, and other third parties) may file a Certificate Revocation Request in order to register:

- Complaints related to certificate issuance
- Suspected Private Key compromise
- Certificate misuse
- Other types of fraud, compromise, misuse, or inappropriate conduct related to the certificate.

Non-Subscriber Certificate Revocation Requests must follow the procedures detailed in §4.9.3.

3.4.3 Identification and authentication for revocation requests by other participants in the SSL.com PKI

A revocation request for an SSL.com-issued certificate by any other authorized participant in the SSL.com PKI (such as a Subordinate CA or external RA) shall be identified and/or authenticated by that authorized participant.

Identification and/or authorization for a revocation request must in all cases follow the procedures detailed in §4.9.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This chapter specifies the policy, procedures and requirements for the management of Certificates across the entire life cycle, including:

- Application processing
- Certificate issuance
- Certificate acceptance
- Key pair and certificate usage
- Certificate re-issuance
- Certificate renewal
- Certificate re-key
- Certificate modification
- Certificate revocation and suspension
- Certificate status services
- End of subscription
- Key escrow and recovery

Any request to re-issue a certificate without changing the expiration date (the `validTo` field) and the Subject Information (the `Subject Distinguished Name` field), shall be defined as a "re-issuance" and addressed in §4.2.5.

Any request to re-issue a certificate without changing the Public Key or any other information, with the sole exception of the expiration date (the `validTo` field), shall be defined as a "renewal" and addressed in §4.6.

Any request to change the Key Pair in a certificate shall be defined as "re-keying" and addressed in §4.7. Note that, apart from the Key Pair, any other information (such as the CN, SAN entries, email addresses etc.) may also be changed in the re-key process.

Any request to change any information in a certificate (such as the CN, SAN entries, email addresses etc.), without changing the Public Key, shall be defined as "modification" and addressed in §4.8.

SSL.com's PKI operations follow the Certificate Management Protocol (CMP) as defined in RFC 4210.

4.1 Certificate Application

4.1.1 Who may submit a certificate application

Either the Applicant or an authorized Certificate Requester may submit certificate requests. Applicants are responsible for the accuracy of any data submitted.

In all cases SSL.com or any Enterprise RA shall require identification and authentication sufficient to meet the requirements relevant to the type of certificate requested.

SSL.com shall not issue Certificates to organizations or entities on a government denied list maintained by the United States, or which is located in a country with which the laws of the United States prohibit doing business.

SSL.com shall only issue EV SSL and EV Code Signing Certificates to Applicants which submit a complete Certificate Request and meet the requirements specified in the CA/Browser Forum's EV SSL and EV Code Signing Guidelines respectively, in addition to the requirements of this CP/CPS.

SSL.com shall only issue Mark Certificates to Mark Asserting Entities which submit a complete Certificate Request and meet the requirements specified in the MC Guidelines, in addition to the requirements of this CP/CPS.

4.1.2 Enrollment process and responsibilities

The enrollment process to obtain an SSL.com certificate shall include:

- Applying for a certificate
- Generating a Key Pair (except for requests associated with Mark Certificates)
- Delivering the Public Key of the Key Pair to SSL.com (except for requests associated with Mark Certificates)
- Agreeing to the applicable Subscriber Agreement, and
- Paying any applicable fees

The order in which these events occur may vary, depending on the method used and product ordered.

SSL.com shall obtain any additional documentation and perform any additional steps deemed necessary to meet the requirements for the product requested. EV TLS, EV Code Signing and Mark Certificate requests must fully meet the requirements for those products.

4.1.2.1 Enrollment process for SSL.com central RA

In most cases, a request for an SSL.com certificate is made through the SSL.com Account Dashboard. Any Applicant will be directed to log in to or create an SSL.com account before any request shall be processed. A request submitted via the SSL.com Account Dashboard is identified with the account holder and considered authentic.

SSL.com may, at its sole discretion, and on a case by case basis, accept requests which are not submitted via the Applicant's SSL.com Account. Additional verification and/or authentication may be required for requests submitted outside of the SSL.com Account Dashboard.

The following Applicant roles are required for the issuance of an EV and Mark Certificate.

1. **Certificate Requester:** The EV/Mark Certificate Request must be submitted by an authorized Certificate Requester. A Certificate Requester is a natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV/Mark Certificate Request on behalf of the Applicant.

2. **Certificate Approver:** The EV/Mark Certificate Request must be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV/Mark Certificate Requests submitted by other Certificate Requesters.
3. **Contract Signer:** A Subscriber Agreement applicable to the requested EV/Mark Certificate must be signed by an authorized Contract Signer. A Contract Signer is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.
4. **Applicant Representative:** In the case where SSL.com and the Subscriber are affiliated, Terms of Use applicable to the requested EV/Mark Certificate must be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.

The Applicant may authorize one individual to occupy two or more of these roles, and/or may authorize more than one individual to occupy any of these roles.

In the F2F Verification Procedure required for Mark Certificate requests, either the Contract Signer or the Certificate Approver can act as the Designated Individual.

4.1.2.2 Enrollment process for Enterprise RAs

Any Enterprise RA authorized to use the SSL.com PKI to issue Certificates must have appropriate processes in place to receive certificate requests, as detailed in chapter 3.

Any Enterprise RA authorized to use the SSL.com PKI may submit certificate requests by an authorized call to the SSL.com API.

4.1.2.3 The Certificate Signing Request (CSR)

With the exception of SSL.com generating Key Pairs on behalf of an Applicant as described in §6.2.1, a valid Certificate Signing Request (CSR) must be created and submitted by the Applicant. A valid CSR will be derived from a Key Pair generated by the Applicant or the Applicant's agent. A valid CSR will incorporate the generated Public Key and other such information as is required to create the requested certificate.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The Certificate request may include all factual information about the Applicant to be included in the Certificate, and such additional information as is required for SSL.com to comply with this CP/CPS. In cases where the Certificate request does not contain all the necessary information

about the Applicant, SSL.com shall obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant.

SSL.com maintains systems and processes to authenticate the identity of any Applicant, and follows documented procedures to verify all data requested for inclusion in the Certificate by the Applicant.

In the case of TLS certificates, applicant information MUST include, but is not limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's subjectAltName extension.

Initial identity verification and any additional validation required for specific certificate types shall follow the procedures detailed in Chapter 3.

Successful validation through these identification and authentication procedures must occur prior to issuance of any certificate.

§6.3.2 limits the validity period of Subscriber Certificates.

SSL.com MAY use the documents and data provided in §3.2 to verify certificate information, or may reuse previous validations themselves, provided that SSL.com obtained the data or document from a source specified under §3.2 or completed the validation itself within the maximum number of days prior to issuing the Certificate, as defined in the following table:

Subject Identity Information validation data reuse periods

Certificate issued on or after	Certificate issued before	Maximum data reuse period
	March 15, 2026	825 days
March 15, 2026		398 days

For validation of Domain Names and IP Addresses according to §3.2.2.4 and §3.2.2.5, any data, document, or completed validation used MUST be obtained within the maximum number of days prior to issuing the Certificate, as defined in the following table:

Domain Name and IP Address validation data reuse periods

Certificate issued on or after	Certificate issued before	Maximum data reuse period
	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days
March 15, 2027	March 15, 2029	100 days
March 15, 2029		10 days

As an exception to the validation reuse period defined above, for Mark Certificates face-to-face validation is not required more than once for any Subscriber Organization (or Parent, Subsidiary, or Affiliate) so long as SSL.com has maintained continuous contact with one or more

Subscriber representatives and maintains a system for authorization by the Subscriber of new Subscriber representatives (or representatives of a Parent, Subsidiary, or Affiliate). “Continuous contact” means SSL.com has one or more direct contacts with a Subscriber representative during the validity period of any MC issued to the Subscriber or within 90 days of the expiration of the last of the Subscriber’s MC to expire.

An authorization letter from the owner of record of the Registered Mark or Government Mark (as described in Section 3.2.17.1.2 and Section 3.2.17.2.2 of the MC Requirements) may be reused for up to 1,858 days.

Methods 4, 5 and 7 of §6.2.7.4.1 may be reused if Subscriber Private Key protection has been validated no more than 13 months prior to issuing the Code Signing Certificate.

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

SSL.com shall develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate’s approval, as reasonably necessary to ensure that such requests are properly verified under this CP/CPS. For Code Signing and EV Code Signing Certificates, SSL.com shall determine whether the entity is identified as requesting a Code Signing Certificate from a High Risk Region of Concern

If a Delegated Third Party fulfills any of SSL.com’s obligations under this section, SSL.com shall verify that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as SSL.com’s own processes.

4.2.2 Approval or rejection of certificate applications

Any certificate request which cannot be verified shall be rejected.

SSL.com SHALL NOT issue Certificates containing Internal Names or Reserved IP Addresses, as such names cannot be validated according to Section 3.2.2.4 or Section 3.2.2.5.

Effective 2025-09-15, SSL.com SHALL NOT issue Certificates containing Address and Routing Parameter Area Names.

Effective 2026-03-15, SSL.com SHALL NOT issue Certificates containing Domain Names that end in an IP Reverse Zone Suffix.

SSL.com reserves the right to reject any certificate application for any reason, including but not limited to:

- Correlation with previously revoked Certificates
- Correlation with previously rejected certificate requests
- Presence on a government denied list maintained by the United States or location in a country with which the laws of the United States prohibit doing business

- Insufficient, incorrect or inapplicable supporting documentation

SSL.com may reject the request for any certificate the issuance of which may harm, diminish or otherwise negatively impact SSL.com's business or reputation. SSL.com shall be the sole determinant of what meets these criteria, and is not obligated to provide a reason for rejection of any Certificate Request.

SSL.com shall not issue new or replacement Code Signing Certificates to an entity that SSL.com determined intentionally signed Suspect Code. SSL.com shall keep meta-data about the reason for revoking a Code Signing Certificate as proof that the Code Signing Certificate was not revoked because the Applicant was intentionally signing Suspect Code.

SSL.com MAY issue new or replacement Code Signing Certificates to an entity who is the victim of a documented Takeover Attack, resulting in a loss of control of the Private Key associated with their Code Signing Certificate.

If SSL.com is aware that the Applicant was the victim of a Takeover Attack, SSL.com MUST verify that the Applicant is protecting its Code Signing Private Keys under §6.2.1. SSL.com MUST verify the Applicant's compliance with §6.2.1 (i) through technical means that confirm the Private Keys are protected using the method described in §6.2.1 or (ii) by relying on a report provided by the Applicant that is signed by an auditor who is approved by SSL.com and who has IT and security training.

Documentation of a Takeover Attack MAY include a police report (validated by SSL.com) or public news report that admits that the attack took place. The Subscriber MUST provide a report from an auditor with IT and security training that provides information on how the Subscriber was storing and using Private keys and how the intended solution for better security meets this CP/CPS for improved security.

Except where issuance is expressly authorized by the Application Software Supplier, SSL.com MUST not issue new Code Signing Certificates to an entity where SSL.com is aware that the entity has been the victim of two Takeover Attacks or where SSL.com is aware that entity breached a requirement under this Section to protect Private Keys under Section 6.2.1.

Other than in the cases given above, SSL.com shall approve any successfully validated certificate application which meets the criteria for the certificate requested.

Extended Validation (EV) and Mark Certificate Requests shall require a second validation specialist for final cross-correlation and due diligence before approval, in accordance with Section 3.2.2.13 of the EV Guidelines and Section 3.2.19 of the MC Guidelines respectively. The second validation specialist may require additional documentation and/or verification before authorizing an EV or Mark Certificate. The second validation specialist cannot be the same individual who collected the documentation and originally approved the EV or Mark Certificate. In no case shall an EV or Mark Certificate be validated, authorized or issued by a single validation specialist.

In the case of EV or Mark Certificates to be issued in compliance with the requirements of section 1.3.2 of the EV Guidelines or section 1.3.2 of the MC Guidelines respectively, an Enterprise RA MAY perform the requirements of Final Cross-Correlation and Due Diligence of section 3.2.2.13 of the EV Guidelines or section 3.2.19 of the MC Guidelines respectively.

4.2.3 Time to process certificate applications

SSL.com shall process certificate applications in a commercially reasonable time frame.

SSL.com shall not be responsible for delays in application processing resulting from action or inaction by the Applicant or the Applicant's agent, including omitted or incorrect details and/or documentation in the application.

SSL.com shall not be responsible for events outside of SSL.com's control which delay application processing.

4.2.4 Certificate Authority Authorization (CAA)

SSL.com supports CAA for the issuance of TLS and Mark Certificates as described in §3.2.2.8.

Subscribers who wish to authorize SSL.com to issue TLS Certificates for their FQDNs should include a CAA record property `issue` or `issuewild`, including the value "ssl.com" in their respective DNS zone.

SSL.com has a contractual agreement with Entrust which allows SSL.com to accept Entrust's CAA domain names for issuance authorization. Subscribers who utilize Entrust as a RA and wish to authorize SSL.com to issue TLS Certificates for their Domain Names should include a CAA record property `issue` or `issuewild`, including at least one of the values "entrust.net", or "affirmtrust.com" in their respective DNS zone.

Subscribers who wish to authorize SSL.com to issue Mark Certificates for their FQDNs should include a CAA record property `issuevmc` including the value "ssl.com" in their respective DNS zone.

Subscribers who already have CAA entries with property `issue` or `issuewild` in their respective DNS zone and need a TLS Certificate from SSL.com must add a CAA record property `issue` or `issuewild`, including the value "ssl.com".

Subscribers who already have CAA entries with property `issuevmc` in their respective DNS zone and need a Mark Certificate from SSL.com must add a CAA record property `issuevmc`, including the value "ssl.com".

Starting on March 15, 2025 prior to issuing a Certificate that includes a Mailbox Address, SSL.com SHALL retrieve and process CAA records in accordance with Section 4 of RFC 9495 (Certification Authority Authorization (CAA) Processing for Email Addresses).

When processing CAA records, SSL.com SHALL process the `issuemail` property tag as specified in RFC 9495. Additional property tags MAY be supported, but SHALL NOT conflict with or

supersede the authorizations to issue S/MIME Certificates as specified in the `issuemail` property tag.

If SSL.com issues a Certificate following a CAA check, SSL.com SHALL do so within the TTL of the CAA record, or 8 hours, whichever is greater. This stipulation does not prevent SSL.com from checking CAA records at any other time.

If the Certificate includes more than one Mailbox Address, then SSL.com SHALL perform the above procedure for each Mailbox Address.

CAA checking is optional for Certificates issued by a Technically Constrained Subordinate CA Certificate as set out in §7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Technically Constrained Subordinate CA Applicant.

SSL.com SHALL NOT issue a Certificate unless SSL.com determines that Certificate Request is consistent with the applicable CAA RRset. SSL.com SHALL log all actions taken, if any, consistent with its CAA processing practice.

SSL.com is permitted to treat a record lookup failure as permission to issue if:

- the failure is outside SSL.com's infrastructure; and
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

4.2.5 Re-issuance Requests

In the case of EV SSL and EV Code Signing Certificates, SSL.com may rely on a previously verified certificate request to issue a replacement certificate, so long as the certificate being referenced was not revoked due to fraud or other illegal conduct, if:

1. The expiration date of the replacement certificate is the same as the expiration date of the EV Certificate that is being replaced, and
2. The Subject Information of the Certificate is the same as the Subject in the EV Certificate that is being replaced.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Any RA, internal or external, utilizing SSL.com's PKI shall perform validation of all information sent before issuing any certificate.

Before issuance of a Mark Certificate, SSL.com SHALL log the Mark pre-certificate (including all the data included in the Subject field of the certificate plus the Mark Representation) to one or more public CT logs.

4.3.1.1 Manual authorization of certificate issuance for Root CAs

Certificate issuance by a Root CA shall require an individual authorized by SSL.com (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.1.2 Linting of to-be-signed Certificate content

Due to the complexity involved in implementing Certificate Profiles that conform to the Baseline Requirements, SSL.com SHOULD implement a Linting process to test the technical conformity of each to-be-signed artifact prior to signing it. When a Precertificate has undergone Linting, it is not necessary for the corresponding to-be-signed Certificate to also undergo Linting, provided that SSL.com has a technical control to verify that the to-be-signed Certificate corresponds to the to-be-signed Precertificate in the manner described by RFC 6962, Section 3.2.

Effective 2025-03-15, SSL.com SHALL implement such a Linting process.

Methods used to produce a certificate containing the to-be-signed Certificate content include, but are not limited to:

1. Sign the `tbsCertificate` with a "dummy" Private Key whose Public Key component is not certified by a Certificate that chains to a publicly-trusted CA Certificate; or
2. Specify a static value for the `signature` field of the Certificate ASN.1 SEQUENCE.

SSL.com SHOULD use the Linting tools that have been widely adopted by the industry (see https://cabforum.org/resources/tools/). SSL.com MAY also use its own certificate Linting tools.

4.3.1.3 Linting of issued Certificates

SSL.com MAY use a Linting process to test each issued Certificate.

4.3.2 Notification to Subscriber by the CA of issuance of Certificate

Any RA, internal or external, utilizing SSL.com's PKI shall notify the Subscriber of the successful issuance of a certificate. Notification shall be by email, using an email address provided by the Subscriber. Notification may, at SSL.com's sole discretion, be provided by other means as required.

Notification shall also constitute acknowledgement that the certificate is available for review, access and download from the SSL.com Account Dashboard correlating to the certificate ordered.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The Subscriber or Subscriber's agent is responsible for review and verification of information contained in the issued certificate. The Subscriber or agent shall be deemed to have accepted the certificate:

- By downloading, installing or taking delivery by any other method of the certificate
- After 30 (thirty) days have passed from the communication of fulfillment.

4.4.2 Publication of the certificate by the CA

Any certificate issued by SSL.com shall be published by email to the address corresponding to the Subscriber or agent requesting the certificate.

The certificate may also be published by other means, including:

- Publication to the corresponding SSL.com Account
- Publication to a public repository, such as an x.500 or LDAP repository
- Publication to other entities as required by the SSL.com PKI CP/CPS

4.4.3 Notification of certificate issuance by the CA to other Entities

Any RA, internal or external, may be notified regarding the issuance of a certificate. Notification may include transmission of the certificate by SSL.com as the issuing CA to a corresponding Enterprise RA.

4.5 Key pair and certificate usage

4.5.1 Subscriber Private Key and certificate usage

Subscribers using any certificate issued through the SSL.com PKI are required to protect the Private Key for that certificate, including:

- Securing the Private Key (and any copies made) to prevent disclosure or compromise
- Using the Private Key and/or certificate only as authorized by the relevant terms of service and/or Subscriber Agreement
- Ceasing use of the Private Key after expiration or revocation of the associated certificate
- Contacting the issuing entity if the Private Key is compromised
- Using the certificate only as applicable and for the intended purpose (per the key usage field of that certificate)

Subscribers requesting or utilizing Document Signing, Code Signing or EV Code Signing Certificates must observe the requirements for Private Key generation and protection given in §6.2.1 of this CP/CPS.

Subscriber private keys associated with Mark Certificates do not need to be protected, and may be discarded.

4.5.2 Relying party Public Key and certificate usage

Any party relying on a certificate issued using the SSL.com PKI accepts responsibilities for the use of a Subscriber's Public Key and certificate. These responsibilities include:

- Obligation to rely on the certificate only for applications appropriate for the Certificate type (as set forth in this CP/CPS) and consistent with applicable certificate content (e.g., key usage field)
- Successful performance of Public Key operations as a condition of relying on a certificate
- Assumption of responsibility to check the certificate's status, including using one of the required or permitted mechanisms set forth in this CP/CPS (as referenced in §4.9)
- Assent to the terms of the applicable Relying Party Agreement as a condition of relying on the certificate

4.6 Certificate renewal

For the purposes of this CP/CPS, "certificate renewal" means the issuance of a new certificate without changing the Public Key or any other information used in the original certificate, with the sole exception of the `notAfter` field (i.e. the renewal date).

4.6.1 Circumstance for certificate renewal

Unless otherwise specifically prohibited in this CP/CPS, any certificate issued utilizing the SSL.com PKI may be renewed if the certificate meets the following criteria:

- The original certificate has not been revoked or otherwise flagged
- The Public Key from the original certificate has not been blocklisted
- The Private Key corresponding to the original certificate has not been compromised
- The key lifetime is not exceeded as stated in §6.3.2
- All information within the certificate, other than the `notAfter` field, remains accurate
- The renewed certificate's cryptographic security is deemed to remain sufficient for the certificate's intended lifetime
- The information provided in the request still passes the appropriate validation checks
- No further or additional validation is required beyond repeating the same steps performed originally

Certificates which have either been previously renewed or previously re-keyed may be renewed again so long as the criteria above are met. The original certificate may be revoked after renewal is complete. Revocation after renewal shall be at the sole discretion of SSL.com or the authorized entity utilizing the SSL.com PKI to process the renewal. Regardless of revocation status, the original certificate shall not be further renewed, re-keyed or modified.

4.6.2 Who may request renewal

Renewal of a certificate issued utilizing the SSL.com PKI may be requested by the Subscriber or the Subscriber's agent.

Subscribers with Certificates issued directly by SSL.com may request renewal via their SSL.com Account Dashboard.

Any RA, internal or external, utilizing the SSL.com PKI shall require a specific request for renewal.

Certificates issued by any entity utilizing the SSL.com PKI shall not be automatically renewed.

4.6.3 Processing certificate renewal requests

Renewal requests shall require validation and/or authentication identical to that for a new certificate.

Subscribers with Certificates issued directly by SSL.com may request renewal via their SSL.com Account Dashboard.

Any certificate slated for renewal shall re-use all information in the original request, with the sole exception of the expiration date (the `notAfter` field).

Any certificate slated for renewal which for any reason fails re-verification and/or re-authentication of the certificate shall not be renewed.

Certificates which cannot be renewed may be capable of re-keying as defined and described in §4.7.

4.6.4 Notification of renewed certificate issuance to Subscriber

Any certificate renewed via the SSL.com PKI shall utilize a notification method identical to that for a new certificate, in compliance with §4.4.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

Acceptance of any certificate renewed via the SSL.com PKI shall use the same methods described for a new certificate in §4.4.1.

4.6.6 Publication of the renewal certificate by the CA

Any certificate renewed via the SSL.com PKI may be published via email to the Subscriber using the same methods described for a new certificate in §4.4.2.

4.6.7 Notification of certificate issuance by the CA to other Entities

Notification to other entities may also be performed for any renewed certificate using the same methods described for a new certificate in §4.4.3.

4.7 Certificate re-key

For the purposes of this CP/CPS, “certificate re-keying” means the re-issuance of a certificate which utilizes a new Key Pair.

Other information used in the original certificate may or may not be changed when a certificate is re-keyed.

In all cases where re-keying is requested and/or performed a new Certificate Signing Request (CSR) must be submitted (per §4.1.2.3) to obtain the new Public Key required.

Mark Certificates shall not be re-keyed.

4.7.1 Circumstances for certificate re-key

Any certificate issued utilizing the SSL.com PKI may be re-keyed, unless otherwise specifically prohibited in the SSL.com PKI CP/CPS.

4.7.1.1 Revocation

In certain cases, an original certificate or previously issued certificate must be revoked as a condition of re-keying.

For instance, if the `subject:commonName` or a `subjectAltName:dNSName` field is altered for the following certificate categories with relation to the previously issued certificate, the original certificate must be revoked as a condition of re-keying:

- Basic SSL
- High Assurance SSL
- Premium SSL
- Wildcard SSL
- Enterprise EV SSL

In all other cases, the original certificate may be revoked after re-keying is complete. In these cases, revocation after re-keying shall be at the sole discretion of SSL.com or the authorized entity utilizing the SSL.com PKI to process the re-key request.

4.7.1.2 Loss, theft or compromise

Any Subscriber, agent or authorized entity utilizing the SSL.com PKI to create a certificate whose Private Key has been stolen, lost or otherwise compromised should immediately request re-keying of that certificate.

The Subscriber should also request revocation of the Public Key that is associated with the lost, stolen or compromised Private Key.

For Server Certificates, if the Subscriber requests that SSL.com revoke a Certificate for the reason of Key Compromise, and has not previously demonstrated and cannot currently

demonstrate possession of the associated Private Key of the Certificate, SSL.com MAY revoke all certificates associated with that Subscriber that contain that Public Key. SSL.com SHALL NOT assume that it has evidence of Private Key compromise for the purposes of revoking the certificates of other subscribers, but MAY block issuance of future certificates with that key.

SSL.com is not responsible for loss, damages or injury resulting from any compromise of a Private Key. Reference should be made to the Subscriber Agreement and/or Relying Party Agreement applicable to the certificate for more information regarding compromised Private Keys.

4.7.1.3 Key pair expiration

Any expired certificate issued from a Key Pair whose usage period has also expired must be re-keyed, unless otherwise specifically prohibited in the SSL.com CP/CPS.

4.7.2 Who may request certification of a new Public Key

Re-keying of a certificate issued via the SSL.com PKI may be requested by the Subscriber or the Subscriber's agent.

Subscribers with Certificates issued directly by SSL.com may request re-keying directly via their SSL.com Account Dashboard.

Any RA, internal or external, utilizing the SSL.com PKI may request a certificate re-key if compromise of that certificate's Private Key is known or suspected to have occurred. This re-keying shall occur at the discretion of SSL.com and/or the internal or Enterprise RA concerned.

4.7.3 Processing certificate re-keying requests

Re-keying requests must be accompanied by a new CSR.

Any certificate slated for re-keying may be re-issued using any or all information in the original request, with the exception of the Public Key and the date of issuance date (the `validFrom` field).

Other information may be changed in a re-key request, as requested by the Subscriber or the Authorized Entity requesting the re-key.

Re-keying requests shall require validation and/or authentication, as described in §4.2.

Any certificate submitted for re-keying which for any reason fails verification and/or authentication shall not be issued.

4.7.4 Notification of new certificate issuance to Subscriber

Any certificate re-keyed via the SSL.com PKI shall utilize a notification method which is in compliance with Section 4.4.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Acceptance of any certificate re-keyed via the SSL.com PKI shall use the same methods described for a new certificate in §4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

Any certificate re-keyed via the SSL.com PKI may be published via email to the Subscriber using the same methods described for a new certificate in §4.4.2.

4.7.7 Notification of certificate issuance by the CA to other Entities

Notification to other entities may also be performed for any re-keyed certificate using the same methods as described in §4.4.3

4.8 Certificate modification

For the purposes of the SSL.com CP/CPS, "certificate modification" means the issuance of a new certificate in which non-essential information has changed, without changing the Key Pair related to the original certificate.

4.8.1 Circumstance for certificate modification

Certificate modification may be requested by a Subscriber when non-essential attributes change, including but not limited to:

- Country change
- Role change
- Address change
- A reorganization resulting in alteration of a DN

Any re-issuance of a certificate in which information other than the Key Pair changes, shall be considered certificate modification. The original Certificate may be revoked after modification is complete, but the original Certificate shall not be further renewed, re-keyed or modified.

4.8.2 Who may request certificate modification

Modification of a certificate issued via the SSL.com PKI may be requested by the Subscriber or the Subscriber's agent.

Subscribers with Certificates issued directly by SSL.com may request modification directly via their SSL.com Account Dashboard.

4.8.3 Processing certificate modification requests

Modification requests shall require validation and/or authentication, as described in §4.2. Any certificate slated for modification which for any reason fails verification and/or authentication of the certificate shall not be renewed.

4.8.4 Notification of modified certificate issuance to Subscriber

Any certificate modified via the SSL.com PKI shall utilize a notification method which is in compliance with Section 4.4.2.

4.8.5 Conduct constituting acceptance of modified certificate

Acceptance of any certificate modified via the SSL.com PKI shall use the same methods described for a new certificate in §4.4.1.

4.8.6 Publication of the modified certificate by the CA

Any certificate modified via the SSL.com PKI may be published via email to the Subscriber using the same methods described for a new certificate in §4.4.2.

4.8.7 Notification of modified certificate issuance by the CA to other Entities

Notification to other entities may also be performed for any modified certificate using the same methods as described in §4.4.3.

4.9 Certificate revocation and suspension

For the purposes of the SSL.com CP/CPS, "revocation" is defined as adding the serial number of a certificate issued via the SSL.com PKI to a Certificate Revocation List (CRL), an Online Certificate Status Protocol (OSCP) and any other relevant database used for blocklisting.

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

Mark Certificates need not be revoked if their unused Private Key suffers a Key Compromise.

SSL.com MAY support revocation of Short-lived Subscriber Certificates.

With the exception of Short-lived Subscriber Certificates, SSL.com SHALL revoke a TLS or Code Signing Certificate within 24 hours and use the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

1. The Subscriber requests in writing that SSL.com revoke the Certificate
    a. specifying a CRLreason of
        - keyCompromise (CRLReason #1) (e.g. the Subscriber's Private Key is suspected of compromise);
        - cessationOfOperation (CRLReason #5) (e.g. the Subscriber will no longer be using the Certificate because they are discontinuing their website);
        - affiliationChanged (CRLReason #3) (e.g. identifying information about the Subscriber in the Certificate has changed); or
        - superseded (CRLReason #4) (e.g. the Subscriber requests a new certificate to replace an existing certificate);

b. without specifying a CRLreason, which leads to CRLReason “unspecified (0)” which results in no reasonCode extension being provided in the CRL;

If the Subscriber requests revocation for Key Compromise and cannot demonstrate possession of the associated Private Key of that Certificate, then SSL.com MAY revoke all certificates associated with that Subscriber that contain that Public Key. SSL.com MUST NOT assume that it has evidence of Key Compromise for the purposes of revoking the Certificates of other Subscribers, but MAY block issuance of future certificates with that key;

2. The Subscriber notifies SSL.com that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. SSL.com obtains evidence that the Subscriber’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. SSL.com is made aware of a demonstrated or proven method that can easily compute the Subscriber’s Private Key based on the Public Key in the Certificate, including but not limited to those identified in Section 6.1.1.2(5) (CRLReason #1, keyCompromise);
5. SSL.com is made aware of a demonstrated or proven method that exposes the Subscriber’s Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise);
6. SSL.com obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address or email address in the Certificate should not be relied upon (CRLReason #4, superseded).
7. SSL.com has reasonable assurance that the Certificate was used to sign Suspect Code (CRLReason #9, privilegeWithdrawn).

With the exception of Short-lived Subscriber Certificates, SSL.com SHOULD revoke a certificate within 24 hours and SHALL revoke a Certificate within 5 days and use the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of §6.1.5 and §6.1.6 (CRLReason #4, superseded);
2. SSL.com obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
3. SSL.com is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);
4. SSL.com is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address or email address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant’s right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);

5. SSL.com is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
6. SSL.com is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
7. SSL.com is made aware that the Certificate was not issued in accordance with the applicable requirements or this CP/CPS or an applicable alternate CPS (CRLReason #4, superseded);
8. SSL.com determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
9. SSL.com's right to issue Certificates is revoked or terminated, unless SSL.com has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
10. Revocation is required by SSL.com's CP/CPS for a reason that is not otherwise required to be specified by section 4.9.1.1 of the Baseline Requirements or section 4.9.1.1 of the Code Signing Baseline Requirements (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or
11. SSL.com receives a lawful and binding ruling from a Government or regulatory body to revoke the Certificate (CRLReason #9, privilegeWithdrawn).
12. For Mark Certificates SSL.com receives a Court Order of Infringement, confirms the authenticity of the Court Order of Infringement, and provides 3 business days notice to the Subscriber that the MC will be revoked.

SSL.com MAY delay revocation of a Code Signing Certificate based on a request from Application Software Suppliers where immediate revocation has a potentially large negative impact to the ecosystem.

When SSL.com obtains verifiable evidence of Key Compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, SSL.com SHOULD update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension. Additionally, SSL.com SHOULD update the revocation date in a CRL entry when it is determined that the Private Key of the Certificate was compromised prior to the revocation date that is indicated in the CRL entry for that Certificate.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

SSL.com SHALL revoke a Subordinate CA Certificate within seven (7) days, if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies SSL.com that the original certificate request was not authorized and does not retroactively grant authorization;
3. SSL.com obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of §6.1.5 and §6.1.6,

4. SSL.com obtains evidence that the Certificate was misused;
5. SSL.com is made aware that the Certificate was not issued in compliance with the applicable requirements or this CP/CPS or an applicable alternate CPS;
6. SSL.com determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. SSL.com or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. SSL.com's or Subordinate CA's right to issue Certificates under the applicable requirements and this CP/CPS expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by SSL.com's CP/CPS.
10. SSL.com receives a lawful and binding ruling from a Government or regulatory body to revoke a CA Certificate.

Applicable revocation reasons (per RFC 5280 and ITU-T X.509) for CA Certificates, are:

- **cACompromise** is used in revoking a CA certificate; it indicates that it is known or suspected that the subject's private key, or other aspects of the subject validated in the CA certificate, have been compromised.
- **affiliationChanged** indicates that the subject's name or other information in the public-key certificate has been modified but there is no cause to suspect that the private key has been compromised.
- **superseded** indicates that the public-key certificate has been superseded but there is no cause to suspect that the private key has been compromised.
- **cessationOfOperation** indicates that the public-key certificate is no longer needed for the purpose for which it was issued but there is no cause to suspect that the private key has been compromised.
- **privilegeWithdrawn** indicates that a public-key certificate was revoked because a privilege contained within that public-key certificate has been withdrawn.

4.9.2 Who can request revocation

Revocation of a certificate issued utilizing the SSL.com PKI may be requested by the Subscriber or the Subscriber's agent. Any RA, internal or external, utilizing the SSL.com PKI may request revocation of a certificate.

Non-Subscribers who wish to request revocation due to reasons which meet one or more of the criteria given in §4.9.1 may file a Certificate Problem Report, as described in §3.4.2 and §4.9.3.3.

4.9.3 Procedure for revocation request

Revocation may be initiated by submitting a request to the appropriate RA (internal or external). A Subscriber can submit a revocation request via an email account associated with

the corresponding SSL.com certificate order. Other approved methods of communication may be allowed, provided that corresponding account credentials are sufficiently presented.

SSL.com shall maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

Relying Parties, Application Software Suppliers, and other non-Subscribers may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates and request certificate revocation as described in §4.9.3.3.

4.9.3.1 Revocation requested by Subscriber or Subscriber's agent

SSL.com shall respond within 24 hours to a Subscriber's valid revocation request. A valid revocation request is one in which the corresponding account credentials, in conjunction with one or more of the criteria outlined in §4.9.1, are sufficiently presented.

For Server Certificates, if a Subscriber requesting revocation for the reason of Key Compromise has previously demonstrated or can currently demonstrate possession of the private key of the certificate as described in §4.9.12, then SSL.com SHALL revoke all non-expired Server Certificates associated with that key across all Subscribers.

4.9.3.2 Revocation Requested by an Enterprise RA

Any authorized Enterprise RA utilizing the SSL.com PKI may request revocation of a certificate only if proper credentials are presented. Should the request meet any of the criteria given in §4.9.1, along with approved account credentials, SSL.com CA shall complete the revocation.

For any revocation request received from an External RA, SSL.com shall provide a signed acknowledgement of the request and confirmation of actions to the requesting RA.

4.9.3.3 Revocation requested by Non-Subscribers

Relying Parties, Application Software Suppliers, and other non-Subscribers seeking to request revocation of a Certificate will find instructions for filing a Certificate Problem Report at https://www.ssl.com/revoke. Certificate Problem Reports should be filed to report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. SSL.com shall proceed with the revocation process if the request meets any of the scenarios described in §3.4.2 and/or §4.9.1.1.

For Server Certificates, if anyone requesting revocation for the reason of Key Compromise has previously demonstrated or can currently demonstrate possession of the private key of the certificate as described in §4.9.12, then SSL.com SHALL revoke all non-expired Server Certificates associated with that key across all Subscribers.

4.9.3.4 Revocation requested by an Application Software Supplier

If an Application Software Supplier requests SSL.com to revoke a Certificate because the Application Software Supplier believes that a Certificate attribute is deceptive, or that the Certificate is being used for malware, bundle ware, unwanted software, or some other illicit purpose, then the Application Software Supplier may request that SSL.com revoke the certificate.

Within two (2) business days of receipt of the request, SSL.com MUST either revoke the certificate or inform the Application Software Supplier that it is conducting an investigation.

If SSL.com decides to conduct an investigation, it MUST inform the Application Software Supplier whether or not it will revoke the Certificate, within two (2) business days.

If SSL.com decides that the revocation will have an unreasonable impact on its customer, then SSL.com MUST propose an alternative course of action to the Application Software Supplier based on its investigation.

4.9.4 Revocation request grace period

The grace period given for TLS certificates is the maximum allowed by the CA/B Forum Baseline Requirements.

For all incidents involving malware, SSL.com SHALL revoke the Code Signing Certificate in accordance with and within the following maximum timeframes. Nothing herein prohibits SSL.com from revoking a Code Signing Certificate prior to these timeframes.

1. SSL.com SHALL contact the software publisher within one (1) business day after SSL.com is made aware of the incident.
2. SSL.com SHALL determine the volume of relying parties that are impacted (e.g., based on OCSP logs) within 72 hours after being made aware of the incident.
3. SSL.com SHALL request the software publisher send an acknowledgement to SSL.com within 72 hours of receipt of the request.
    a. If the publisher responds within 72 hours, SSL.com and publisher SHALL determine a “reasonable date” to revoke the certificate based on discussions with SSL.com.
    b. If the publisher does NOT respond within 72 hours, SSL.com SHALL notify the publisher that SSL.com will revoke the certificate in 7 days if no further response is received.
        i. If the publisher responds within 7 days, SSL.com and the publisher will determine a “reasonable date” to revoke the certificate based on discussion with SSL.com.
        ii. If the publisher does NOT respond after 7 days, SSL.com SHALL revoke the certificate, except if SSL.com has documented proof (e.g., OCSP logs) that this will cause significant impact to the general public.

4.9.4.1 Code Signing Certificate revocation dates

When revocation of a Code Signing Subscriber Certificate is done due to a Key Compromise or use in Suspect Code SSL.com SHALL determine an appropriate value for the revocationDate based on its own investigation. SSL.com SHALL set a historic date as revocationDate if deemed appropriate.

More specifically:

1. A Certificate MAY have a one-to-one relationship or one-to-many relationship with the signed Code. Regardless, revocation of a Certificate may invalidate the Code Signatures on all signed Code, some of which could be perfectly sound. Because of this, after working with the Subscriber, SSL.com MAY specify the time at which the Certificate is first considered to be invalid in the `revocationDate` field of a CRL entry or the `revocationTime` field of an OCSP response to time-bind the set of software affected by the revocation, and software should continue to treat objects containing a timestamp dated before the revocation date as valid. This is called a back dated revocation and applies only to signing Certificates.
2. Backdating the revocationDate field is an exception to best practice described in RFC 5280 (section 5.3.2); however, the Code Signing Baseline Requirements specify the use of the `revocationDate` field to convey the "invalidity date" to support Application Software Supplier software implementations that process the `revocationDate` field as the date when the Certificate is first considered to be invalid.
3. SSL.com reserves the right to back date a revocation of signing certificates to nullify any trust applied to Code signed with those certificates, for reasons described in §4.9.1.1, including the violation of material obligations established in the Subscriber Agreement (e.g. non-payment, dispute or chargeback of payment, breach of financial obligations, or other payment disputes resulting in a refund of fees associated with the certificate lifespan).
4. If a Code Signing Certificate previously has been revoked, and the SSL.com later becomes aware of a more appropriate revocation date, then SSL.com MAY use that revocation date in subsequent CRL entries and OCSP responses for that Code Signing Certificate.

4.9.5 Time within which CA must process the revocation request

SSL.com SHALL provide a preliminary report on its findings within 24 hours after receiving a Certificate Problem Report to both the Subscriber and the entity who filed the Certificate Problem Report.

Based on these findings, SSL.com SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date upon which SSL.com will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in §4.9.1.1.

SSL.com SHALL determine whether revocation or other appropriate action is warranted and set a revocation date based on at least the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Report received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
5. Relevant legislation.

4.9.6 Revocation checking requirement for relying parties

Relying parties should validate the authenticity and intended usage of a Certificate using the resources described in §4.10.1.

4.9.7 CRL issuance frequency

Within **twenty-four (24) hours** of issuing its first Certificate, the Issuing CA SHALL generate and publish either:

- a full and complete CRL; OR
- partitioned (i.e., "sharded") CRLs that, when aggregated, represent the equivalent of a full and complete CRL.

For CAs issuing Subscriber Certificates:

- A new CRL SHALL be updated and published at least every:
    - **seven (7) days** if all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod ("AIA OCSP pointer"); or
    - **four (4) days** in all other cases;
- A new CRL SHALL be updated and published within **twenty-four (24) hours** after recording a Certificate as revoked.
- The value of the `nextUpdate` field of the CRL SHALL NOT be more than **ten (10) days** beyond the value of the `thisUpdate` field.

For the status of Code Signing Certificates, SSL.com SHALL publish a CRL then it SHALL be updated and reissued at least once every **seven (7) days**, and the value of the `nextUpdate` field SHALL NOT be more than **ten (10) days** beyond the value of the `thisUpdate` field.

For the status of NAESB Subscriber Certificates, the CRL SHALL be updated and reissued at least once every **twenty-four (24) hours**, and the value of the `nextUpdate` field SHALL NOT be more than **ten (10) days** beyond the value of the `thisUpdate` field.

For CAs issuing CA Certificates:

- A new CRL SHALL be updated and published at least every **twelve (12) months**;
- A new CRL SHALL be updated and published SHALL be updated and published within **twenty-four (24) hours** after recording a Certificate as revoked.
- The value of the `nextUpdate` field of the CRL SHALL NOT be more than **twelve (12) months** beyond the value of the `thisUpdate` field.

For the status of CA Certificates issuing NAESB Subscriber Certificates, SSL.com SHALL update and reissue CRLs at least:

- once every **six (6) months** and
- within **three (3) hours** after revoking a NAESB Issuing Subordinate CA Certificate,

and the value of the `nextUpdate` field SHALL NOT be more than **twelve (12) months** beyond the value of the `thisUpdate` field.

Under normal conditions, SSL.com posts new entries to the CRL as soon as a revocation request is confirmed.

For TLS Certificates, SSL.com SHALL continue issuing CRLs until one of the following is true: - all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; OR - the corresponding Subordinate CA Private Key is destroyed.

For Code Signing, EV Code Signing, Document Signing and Timestamp Certificate, SSL.com SHALL provide accurate and up-to-date revocation status information for a period not less than **ten (10) years** beyond expiry of a Certificate (see also 4.10.1). After the expiration of a Code Signing or Timestamp Issuing CA, the associated CRLs SHALL remain published for at least **five (5) years** beyond the expiry of that Issuing CA.

4.9.8 Maximum latency for CRLs

Where applicable, the maximum latency for the Certificate Revocation List is ten (10) minutes.

4.9.9 On-line revocation/status checking availability

The validity interval of an OCSP response is the difference in time between the `thisUpdate` and `nextUpdate` field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

A certificate serial is “assigned” if:

- a Certificate or Precertificate with that serial number has been issued by the Issuing CA; or
- a Precertificate with that serial number has been issued by a Precertificate Signing Certificate, as defined in Section 7.1.2.4 of the Baseline Requirements, associated with the Issuing CA.

A certificate serial is “unassigned” if it is not “assigned”.

The following SHALL apply for communicating the status of Certificates and Precertificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod.

OCSP responders operated by SSL.com SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019. The CA MAY process the Nonce extension (`1.3.6.1.5.5.7.48.1.2`) in accordance with RFC 8954.

For the status of a Subscriber Certificate or its corresponding Precertificate:

- An authoritative OCSP response MUST be available (i.e. the responder MUST NOT respond with the “unknown” status) starting no more than 15 minutes after the Certificate or Precertificate is first published or otherwise made available.
- For OCSP responses with validity intervals less than sixteen hours, SSL.com SHALL provide an updated OCSP response prior to one-half of the validity period before the nextUpdate.
- For OCSP responses with validity intervals greater than or equal to sixteen hours, SSL.com SHALL provide an updated OCSP response at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of a Subordinate CA Certificate, SSL.com SHALL provide an updated OCSP response at least every twelve months, and within 24 hours after revoking the Certificate.

The following SHALL apply for communicating the status of *all* Certificates for which an OCSP responder is willing or required to respond.

OCSP responses MUST conform to RFC6960 and/or RFC5019. OCSP responses MUST either:

1. be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. be signed by an OCSP Responder which complies with the OCSP Responder Certificate Profile in Section 7.1.2.8 of the Baseline Requirements.

OCSP responses for Subscriber Certificates MUST have a validity interval greater than or equal to eight hours and less than or equal to ten days.

If the OCSP responder receives a request for the status of a certificate serial number that is “unassigned”, then the responder SHOULD NOT respond with a “good” status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.2.3 or Section 7.1.2.5 of the Baseline Requirements, the responder MUST NOT respond with a “good” status for such requests.

4.9.10 On-line revocation checking requirements

No stipulation

4.9.11 Other forms of revocation advertisements available

Because some Application Software Suppliers utilize non-standard revocation mechanisms, SSL.com SHALL, if requested by the Application Software Supplier and using a method of communication specified by the Application Software Vendor, notify the Application Software Supplier whenever SSL.com revokes a Code Signing Certificate because

1. the CA mis-issued the Certificate,
2. the Certificate was used to sign Suspect Code, or
3. there is a suspected or actual compromise of the Applicant's or CA's Private Key.

4.9.12 Special requirements regarding key compromise

Third parties must use the Certificate Problem report process, as described in §3.4.2 and may follow at least one of the following methods to demonstrate that a Private Key is indeed Compromised:

1. Submission of the private key itself;

2. Submission of a signed CSR with a Common Name indicating that the key is compromised e.g. "This key is compromised". This CSR can be generated using the following OpenSSL command:

```
openssl req -new -key privkey.pem -subj "/CN=This key is compromised/" -out p
roofofcompromise.csr
```

3. Submission of signed data indicating that the key is compromised e.g. "This key is compromised" by following the instructions at Proving Possession of a Private Key.

4.9.13 Circumstances for suspension

The SSL.com PKI does not support Certificate suspension.

4.9.14 Who can request suspension

No entity is permitted to request suspension of any Certificate issued utilizing the SSL.com PKI.

4.9.15 Procedure for suspension request

Certificate suspension is not provided.

4.9.16 Limits on suspension period

Certificate suspension is not provided.

4.10 Certificate status services

SSL.com shall maintain services to provide certificate status information for any certificate issued by the SSL.com PKI.

4.10.1 Operational characteristics

CRLs SHALL be available via a publicly-accessible HTTP URL (i.e., “published”).

If SSL.com provides OCSP responses for Code Signing, EV Code Signing, Document Signing and Timestamp Certificates, then it shall provide them beyond expiry of such a Certificate which MAY be at least ten (10) years after the expiration of the certificate. Application Software Suppliers MAY request SSL.com to support a longer life-time according to their trust store requirements.

If a Code Signing Certificate contains the Lifetime Signing OID, the digital signature becomes invalid when the Code Signing Certificate expires, even if the digital signature is timestamped.

SSL.com CAs shall include URLs to revocation information within any issued Certificate in `CRL Distribution Points` (where applicable) and `Authority Information Access` extensions.

4.10.2 Service availability

SSL.com shall operate and maintain its CRL and optional OCSP capability with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

SSL.com shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by SSL.com.

SSL.com shall maintain 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 any Certificate which is the subject of such a complaint.

4.10.3 Optional features

No stipulation

4.11 End of subscription

Subscribers have two options in terms of ending a certificate subscription. A certificate subscription is deemed to end when the certificate:

1. is revoked prior to the date found in the `validTo` field, or
2. reaches the `validTo` date and expires.

Either of these options shall result in the termination of subscription. SSL.com, or the appropriate Authorized Third Party or Enterprise RA, shall notify a Subscriber of the need for renewal prior to the expiration of any certificate issued via the SSL.com PKI. Notifications can be configured through the Subscriber’s SSL.com Account.

4.12 Key escrow and recovery

The SSL.com PKI does not support key escrow.

4.12.1 Key escrow and recovery policy and practices

The SSL.com PKI does not support key escrow.

4.12.2 Session key encapsulation and recovery policy and practices

The SSL.com PKI does not support key escrow.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

SSL.com implements and maintains a comprehensive security program to protect Certificate Data and all aspects of the Certificate Management Process.

SSL.com's security plan is based on an annual risk assessment designed to identify and assess threats and to implement appropriate steps to address these threats.

5.1 Physical controls

SSL.com implements and maintains physical security controls to restrict access to the hardware and software used for SSL.com PKI operations.

5.1.1 Site location and construction

SSL.com operates from a secure commercial datacenter. All critical facilities are housed in secure areas with appropriate security barriers and entry controls. These are protected from unauthorized access, damage and/or interference.

5.1.2 Physical access

SSL.com equipment is physically secured and protected from unauthorized access.

Measures to secure datacenter equipment include two-factor access control through physical cards and biometric readers, 24-hour video surveillance and full-time human security presence which monitors and logs all access.

Support and vetting rooms where RA functions are performed are secured by controlled access and keyed-lock doors. Access card use is logged by the building security system. Video monitoring is employed to record all access to the location. Unauthorized personnel needing to enter into the physical location of a secure datacenter or the area where RA functions are performed shall never be left without oversight by an authorized person.

5.1.3 Power and air conditioning

SSL.com equipment is maintained in a facility which utilizes uninterrupted power supply (UPS) units and automatic backup generators to ensure multiple redundant power sources.

HVAC systems for heating, cooling and ventilation are sufficient to support the operation of the CA system.

5.1.4 Water exposures

SSL.com equipment is maintained in a facility which provides protection against water exposures.

5.1.5 Fire prevention and protection

SSL.com equipment is maintained in a facility equipped with automatic engineered fire suppression systems designed to preserve electronic equipment.

5.1.6 Media storage

Any media used by SSL.com is securely handled and stored to protect it from damage, theft and unauthorized access.

Media containing Private Key material is handled, packaged and stored in a manner compliant with the requirements for the sensitivity level of the information it protects or to which it provides access. Storage protection of CA Private Key material shall be consistent with stipulations in §5.1.2.

5.1.7 Waste disposal

Paper documents or any other printed material containing SSL.com PKI information or related confidential information are securely disposed of by shredding or destruction by an approved service. Removable media containing SSL.com PKI information or related confidential information are securely disposed of by complete destruction of the media, or by the use of an approved utility to wipe or overwrite removable media.

5.1.8 Off-site backup

An off-site location is used for the storage and retention of SSL.com PKI backup software and data. The off-site storage facility is available to authorized personnel 24 hours per day 7 days per week for the purpose of retrieving software and data. The off-site storage facility has appropriate levels of physical security in place and is protected against fire and unauthorized access.

5.2 Procedural controls

5.2.1 Trusted roles

PKI functions are performed by individuals working within clearly defined trusted roles. These trusted roles are established and maintained to share responsibility, limit the ability for action by individual participants, and securely separate duties and functions within the PKI. Trusted roles include but are not limited to:

- **CA Administrator:** Authorized to install, configure and maintain the CA systems used for Certificate life-cycle management.
- **RA Administrator:** Certificate generation and revocation, and end entity creation and deletion
- **System Administrator:** Responsible for operating the CA and RA systems on a day-to-day basis.
- **Network Administrator:** Responsible for operating networking equipment on a day-to-day basis.
- **Vetting Agent:** Responsible for validating the authenticity and integrity of data to be included within Certificates via a suitable RA system
- **Security Auditor** Responsible for internal auditing of CAs and RAs and responsible for administering the implementation of the security practices. This sensitive role shall be free from conflict of interest that might prejudice the impartiality of their duties, e.g. a person assigned with the Security Auditor role shall not audit operations performed partially or entirely by the same person. Security Auditors shall review, maintain, and archive audit logs, and perform or oversee internal audits (independent of formal compliance audits) to ensure that CAs and RAs are operating in accordance with any applicable CP/CPS.

5.2.2 Number of persons required per task

PKI-sensitive operations shall require active participation by SSL.com personnel. This participation shall require at least two trusted individuals to perform the required duties of their specified roles.

CA Private Keys shall be backed up, stored, and recovered only by personnel in Trusted Roles using, at least, dual control in a physically secured environment.

With the exception of audit functions, multi-party control shall not be achieved using personnel that operate under the Security Auditor role. The following tasks shall require two or more persons:

- Generation, activation, and backup of CA keys
- Performance of CA administration or maintenance tasks
- Archiving or deleting CA audit logs. At least one of the participants shall serve in the Security Auditor role
- Physical access to CA equipment
- Access to any copy of the CA cryptographic module

Systems used to process and approve EV Certificate Requests shall require actions by at least two persons in Trusted Roles before issuing an EV Certificate.

5.2.3 Identification and authentication for each role

All individuals authorized in trusted roles must properly authenticate themselves to the relevant CA or RA before performing their duties.

5.2.4 Roles requiring separation of duties

Any trusted role as defined in 5.2.1 intrinsically possesses duties and/or capabilities separate from those in other trusted roles.

As described in 5.2.2, validation of EV certificate requests shall require the participation of at least two validation specialists. For example, one Validation Specialist may review and verify all the Applicant information and a second Validation Specialist may approve issuance of the EV Certificate.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

SSL.com verifies the identity and trustworthiness of all personnel, whether as an employee, agent, or an independent contractor, prior to the engagement of such person(s).

Any personnel occupying a trusted role (as defined in 5.2.1) must possess suitable experience and be deemed qualified by SSL.com.

5.3.2 Background check procedures

All individuals performing trusted role functions have cleared current SSL.com security screenings or background checks appropriate for that role. Background check procedures verify information relevant to the role and may include identity verification (through government-issued photo), as well as examination of one's public record (through research of previous employment history, relevant qualifications and criminal records).

5.3.3 Training requirements

Personnel in trusted roles shall undergo SSL.com training prior to performing any duties as part of that role.

SSL.com shall provide comprehensive training to all personnel performing information verification duties with skills-training that covers:

- Basic Public Key Infrastructure knowledge
- Authentication and vetting policies and procedures (including SSL.com's CP/CPS)
- Common threats to the information verification process (including phishing and other social engineering tactics).

SSL.com shall ensure that all personnel performing validation duties be trained to and maintain an appropriate skill level. Training shall include an initial examination and periodic retraining as required to reflect changes in PKI operations. All training shall be thoroughly documented.

Training for personnel involved in issuance of EV Certificates shall include an internal examination reflecting the EV Certificate validation criteria.

5.3.4 Retraining frequency and requirements

All personnel occupying any Trusted Role shall maintain skill levels consistent with that Trusted Role and shall undergo periodic retraining related to that Role. SSL.com's retraining programs shall reflect and address any relevant changes to the SSL.com PKI and related operations.

SSL.com shall maintain records of all retraining performed.

5.3.5 Job rotation frequency and sequence

SSL.com shall ensure that changes in personnel, including changes in personnel occupying Trusted Roles, shall not affect the operations, services and/or security of the SSL.com PKI and related functions.

5.3.6 Sanctions for unauthorized actions

SSL.com employees and agents failing to comply with the SSL.com CP/CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions.

Any SSL.com employee holding a Trusted Role shall be immediately removed from that role following identification of any unauthorized actions.

SSL.com management will review the underlying details of an incident and promptly issue an applicable resolution report once a conclusion has been reached.

Resolution may result in termination, other sanctions, and/or demotion to a new non-trusted role within the SSL.com PKI.

Resolution may also require retained personnel to undergo additional training programs as determined by SSL.com management.

5.3.7 Independent contractor requirements

Any independent contractor or Delegated Third Party's personnel involved in the issuance of a Certificate via the SSL.com PKI shall be fully subject to the SSL.com's CP/CPS, including training and skills requirements (Section 5.3.3), sanctions (5.3.6), document retention and event logging requirements (5.4.1).

5.3.8 Documentation supplied to personnel

SSL.com shall provide authorized personnel with any relevant documentation needed to carry out job functions or duties. All documentation required for duties, functions and obligations for any personnel utilizing the SSL.com PKI and related functions shall be available to authorized personnel and properly maintained/updated.

Documentation which accurately reflects current operations and processes shall be made readily available.

Access to documentation related to specific Trusted Roles may be limited to personnel occupying those roles.

Relevant materials are systematically disseminated through SSL.com's training and retraining programs.

Any changes to operations, processes or practices related to the SSL.com PKI shall be recorded and reflected in the related documentation.

5.4 Audit logging procedures

5.4.1 Types of events recorded

All events relating to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems of SSL.com and of each Delegated Third Party are recorded in audit log files.

Security audit logs shall be automatically generated whenever possible. Where this is not an option, a logbook, paper form, or other physical mechanism shall be used.

All security audit logs are retained (per §5.4.3 and §5.5) and made available to Qualified Auditors as requested.

Log entries include at least the following elements:

1. Date and time of event;
2. Identity of the person making the journal entry (when applicable); and
3. Description of the event.

5.4.1.1 Types of events recorded for publicly-trusted TLS and Code Signing Certificates

For publicly-trusted TLS and Code Signing Certificates, SSL.com shall record at least the following events:

1. CA certificate and key lifecycle events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction;
    b. Certificate requests, renewal, and re-key requests, and revocation;
    c. Approval and rejection of certificate requests;
    d. Cryptographic device lifecycle management events;

    e. Generation of Certificate Revocation Lists;
    f. Signing of OCSP Responses (as described in §4.9 and §4.10); and
    g. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in the Baseline Requirements and this CP/CPS;
    c. Approval and rejection of certificate requests;
    d. Issuance of Certificates;
    e. Generation of Certificate Revocation Lists; and
    f. Signing of OCSP Responses (as described in §4.9 and §4.10).
    g. Multi-Perspective Issuance Corroboration attempts from each Network Perspective, minimally recording the following information:
        i. an identifier that uniquely identifies the Network Perspective used;
        ii. the attempted domain name and/or IP address; and
        iii. the result of the attempt (e.g., "domain validation pass/fail", "CAA permission/prohibition").
    h. Multi-Perspective Issuance Corroboration quorum results for each attempted domain name or IP address represented in a Certificate request (i.e., "3/4" which should be interpreted as "Three (3) out of four (4) attempted Network Perspectives corroborated the determinations made by the Primary Network Perspective).
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. Installation, update and removal of software on a Certificate System;
    e. System crashes, hardware failures, and other anomalies;
    f. Relevant router and firewall activities (as described in §5.4.1.3); and
    g. Entries to and exits from the CA facility.

5.4.1.2 Types of events recorded for publicly-trusted Time-stamping Certificates

For publicly-trusted Time-stamping Certificates, SSL.com shall record at least the following events:

1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
2. History of the timestamp server configuration,
3. Any attempt to delete or modify timestamp logs,
4. Security events, including:
    a. Successful and unsuccessful Timestamp Authority access attempts;

    b. Timestamp Authority actions performed;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies; and
    e. Firewall and router activities;
5. Revocation of a timestamp certificate,
6. Major changes to the timestamp server's time, and
7. System startup and shutdown.

5.4.1.3 Router and firewall activities logs

Logging of router and firewall activities necessary to meet the requirements of §5.4.1.1, Subsection 3(f) SHALL at a minimum include:

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2 Frequency of processing audit log

SSL.com shall monitor the integrity of the logging processes for application and system logs through continuous automated monitoring and alerting or through a human review to ensure that logging and log-integrity functions are effective. If a human review is utilized and the system is online, the process shall be performed at least once every 31 days.

SSL.com shall monitor audit logs through continuous automated monitoring and alerting or through a human review for possible issues, such as:

- Anomalies and/or irregularities
- Malicious activity

Each review should be reported to the appropriate personnel by summarizing findings, if any.

Investigations which result from reported findings, recommendations made based on these investigations, and actions taken to address reported issues are recorded and made available to auditors as requested.

5.4.3 Retention period for audit log

SSL.com and each Delegated Third Party SHALL retain, for at least two (2) years:

1. CA certificate and key lifecycle management event records (as set forth in §5.4.1.1 (1)) after the later occurrence of:
    a. the destruction of the CA Private Key; or

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

2. Subscriber Certificate lifecycle management event records (as set forth in §5.4.1.1 (2)) after the expiration of the Subscriber Certificate;
3. Timestamp Authority data records (as set forth in §5.4.1.2) after the revocation or renewal of the Timestamp Certificate private key;
4. Any security event records (as set forth in §5.4.1.1 (3)) after the event occurred.

Note: While these Requirements set the minimum retention period, SSL.com MAY choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past audit log events.

5.4.4 Protection of audit log

SSL.com shall collect and regularly analyze relevant audit data for any attempts to violate the integrity of any element of the SSL.com PKI. SSL.com audit logs may be viewed only by authorized personal and auditors.

SSL.com shall decide whether and which audit records may be viewed by others and under what circumstances it shall make those records available.

SSL.com shall protect logs from modification and destruction and maintain digital logs in an encrypted format.

5.4.5 Audit log backup procedures

SSL.com shall perform an onsite backup of the audit log daily. The backup process includes at least a weekly copy of the audit log from the SSL.com facility and storage at a secure, offsite location.

5.4.6 Audit collection system (internal vs. external)

The security audit process shall run independently of the SSL.com PKI certificate issuance software. Security audit processes shall be invoked at system start up and cease only at system shutdown. Security audit processes shall not be capable of being circumvented.

5.4.7 Notification to event-causing subject

SSL.com shall not be required to give any notice to the individual, Organization, device, or application that caused any event which invoked logging.

5.4.8 Vulnerability assessments

SSL.com and Delegated Third Parties perform regular vulnerability assessments and penetration tests (at least once a year) covering all Certificate Systems. These assessments document and implement a vulnerability correction process to identify, review and remediate issues and threats.

Vulnerability assessments may also be performed:

- Within one week of receiving a request from the CA/Browser Forum
- After any system or network changes that the CA determines are significant, and
- At least once per quarter, on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems

Additionally, SSL.com and Delegated Third Parties perform an annual Risk Assessment to:

- Identify foreseeable internal and external 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 SSL.com has in place to counter such threats.

5.5 Records archival

5.5.1 Types of records archived

SSL.com and each Delegated Third Party shall archive all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof.

Additionally, SSL.com and each Delegated Third Party SHALL archive:

1. Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and
2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

SSL.com may also archive other records relating to:

1. CA certificate and key lifecycle
2. Subscriber Certificate lifecycle management
3. Security operations

SSL.com may also archive any other documents deemed relevant to SSL.com PKI operations.

5.5.2 Retention period for archive

Archived audit logs (as set forth in §5.5.1 SHALL be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per §5.4.3, whichever is longer.

Additionally, SSL.com and each Delegated Third Party SHALL retain, for at least two (2) years:

1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in §5.5.1); and
2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in §5.5.1) after the later occurrence of:
    a. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
    b. the expiration of the Subscriber Certificates relying upon such records and documentation.

Note: While these Requirements set the minimum retention period, SSL.com MAY choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past records archived.

For any other archived records, set forth in §5.5.1 (1) to (3), SSL.com shall apply mutatis mutandis the retention rules set forth in §5.4.3.

For any other archived documents deemed relevant to SSL.com PKI operations, set forth in §5.5.1, appropriate retention period shall be applied.

5.5.3 Protection of archive

Archives shall be retained and protected against modification or destruction for the minimum time period specified in §5.5.2.

SSL.com shall take all appropriate measures to ensure that only authorized access is allowed with respect to any archives.

5.5.4 Archive backup procedures

SSL.com shall utilize secure and verifiable backup procedures to provide a complete and readily accessible backup archive in the event of loss or damage to a primary archive.

Any backup archive shall be maintained at a separate, secure location from the primary archive. Access to any backup archive shall employ protections equivalent to the security protocols of its primary archive.

Backup archive maintenance shall include periodic transfer of archived data to new media to prevent data loss.

5.5.5 Requirements for time-stamping of records

All archived documents shall include the date and time of creation, occurrence or modification. The date and time for any document archived shall derive these from a trusted time source as defined in §6.8.

5.5.6 Archive collection system (internal or external)

SSL.com shall employ internal systems to collect and maintain a primary archive.

5.5.7 Procedures to obtain and verify archive information

SSL.com's primary and backup archives shall only be accessible by authorized SSL.com personnel and qualified auditors.

SSL.com may upon request, at its sole discretion, release specific records related to requests by a Subscriber, a Relying Party or an authorized agent of a Subscriber or Relying Party.

SSL.com shall not release archives in their entirety, except as required by law.

SSL.com may require compensation and fees for any costs incurred in accessing or retrieving any requested archival data.

SSL.com shall verify the integrity and readability of primary and backup archives through periodic random testing.

5.6 Key changeover

SSL.com shall ensure a securely managed changeover of Private Keys for any expiring Root Certificate utilized by the SSL.com PKI.

For any key changeover, SSL.com shall maintain, for a temporary and strictly delimited period, concurrent Root Certificates (the original, expiring Root Certificate with the expiring Private Key and the new Root Certificate with the new Private Key) to maintain a seamless transition of functions and services. This period shall end upon the expiration of the original Root Certificate's Private Key.

SSL.com shall provide the new Public Key to Subscribers and Relying Parties through the delivery methods detailed in §6.1.4.

Similar key changeover and key distribution methods shall be employed to manage the expiration of any Cross-Certified Subordinate CA Certificate.

5.7 Compromise and disaster recovery

SSL.com maintains a Business Continuity Plan which details required steps, procedures and actions to restore operations in a timely manner when any function of the SSL.com PKI has been negatively impacted by incidents or disasters.

5.7.1 Incident and compromise handling procedures

5.7.1.1 Incident Response and Disaster Recovery Plans

SSL.com maintains policies and procedures to respond to potential or actual security compromises, natural disasters, and similar events. Documents addressing these needs include

(but are not limited to) an Incident Management Policy (IMP), a Business Continuity and Disaster Recovery Plan and other related resources.

SSL.com shall review, test and update these policies and procedures as needed.

5.7.1.2 Mass Revocation Plans

SSL.com maintains a comprehensive and actionable plan for mass revocation events, performs annual testing of the mass revocation plan, and incorporates lessons learned into such plan in order to continually improve its preparedness for mass revocation events over time.

SSL.com's mass revocation plan includes clearly defined, actionable, and comprehensive procedures designed to ensure rapid, consistent, and reliable response to large-scale certificate revocation scenarios. SSL.com is not required to publicly disclose its mass revocation plan or procedures but MUST make them available to its auditors upon request. SSL.com SHALL annually test, review, and update its plan and such procedures. SSL.com's mass revocation plan MAY be integrated into the SSL.com's incident response, business continuity, disaster recovery, or other similar plans or procedures, provided that provisions governing mass revocation events remain clearly identifiable and satisfy these requirements.

Mass revocation provisions include:

1. Activation criteria – specific, objective, and measurable thresholds at which the mass revocation plan is triggered based on the CA's risk profile, issuance volumes, and operational capabilities;
2. Customer contact information – how subscriber and customer contact details are stored, maintained, and kept up to date;
3. Automation points – processes that are automated or could be automated, and those processes that require manual intervention;
4. Targets and timelines – for incident triage, revocation initiation, certificate replacement, and post-event review;
5. Subscriber notification methods – mechanisms for notifying impacted Subscribers;
6. Role assignments – roles and responsibilities of personnel responsible for initiating, coordinating, and executing the plan;
7. Training and education – training, awareness, and readiness activities for personnel responsible for, or supporting, the plan;
8. Plan testing – annual operational testing to assess readiness and demonstrate implementation feasibility, using one or more of tabletop exercises, simulations, parallel testing, or controlled test environments that DO NOT involve the revocation of active Subscriber Certificates; and
9. Post-test analysis and update schedule – how lessons learned from testing or live incidents are incorporated into the plan, and how often it is reviewed and updated.

5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

SSL.com's Business Continuity Plan includes measures to address any incident in which Computing Resources, Software, and/or Data related to the SSL.com PKI are corrupted. Any affected operations shall be investigated and suspended as required. Any suspended activities shall be restored as quickly as possible commensurate with secure operation of the SSL.com PKI.

The Disaster Recovery Plan shall be tested at least annually.

5.7.3 Recovery Procedures After Key Compromise

SSL.com maintains procedures to address any incident wherein a CA Private Key is lost, destroyed, compromised, or suspected to be compromised. The same applies to the event of a compromise of the algorithms and parameters used to generate the Private Key and certificate. Steps taken after thorough investigation of the incident may include, but are not limited to:

- Revocation of the affected CA Private Key
- Generation of a new CA Key Pair
- Notification of all affected Subscribers
- Revocation of all Certificates signed with the affected CA Private Key

In case of a CA key compromise, SSL.com SHALL notify the relevant Application Software Suppliers without undue delay.

5.7.4 Business continuity capabilities after a disaster

SSL.com's Business Continuity Plan is designed to ensure secure continuous operations, and/or timely and secure restoration of affected operations, in the event of an incident or disaster.

5.8 CA or RA termination

In the event of the termination of any CA and/or RA associated with the SSL.com PKI, SSL.com shall provide timely notice of this information to all affected parties. In addition to prompt notification of termination to the appropriate parties, SSL.com shall:

- Destroy all associated Private Keys
- Revoke all affected unexpired Certificates in existence
- Transfer all responsibilities for the affected CA and/or RA to an entity approved by SSL.com.

In case of a transfer of SSL.com operations to another Trust Service Provider (TSP), a thorough migration plan will be created. All SSL.com Subscribers will receive due notice of this transfer. During the transfer, all critical operations are expected to continue to function properly according to this CP/CPS.

In the event that SSL.com decides upon a full CA business termination, SSL.com will provide a timely notice (including a schedule for business termination) to allow Subscribers and other affected parties to switch to another TSP. When the scheduled termination time is reached, SSL.com will revoke all issued Certificates, update the relevant CRLs and revoke its own root Certificates. Furthermore, it will inform interested third parties (such as Application Software Suppliers) about the end of its operation.

6 TECHNICAL SECURITY CONTROLS

SSL.com shall implement and maintain appropriate technical security controls to govern all operations of the SSL.com PKI.

6.1 Key Pair Generation and Installation

SSL.com shall generate and install all CA Key Pairs in a physically secure environment on secure cryptographic equipment by personnel in trusted roles and using the methodology detailed in §6.1.1.

Access to physical modules shall be controlled as detailed in §6.2.

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

SSL.com CA Key Pairs shall be generated only within cryptographic modules as detailed in §6.2.

SSL.com shall generate CA Key Pairs only by means of a Key Generation Script ceremony. Key pairs and related Certificates are generated by multiple trusted individuals acting in specific trusted roles. The creation of intermediate CA keys is witnessed by an internal or external audit team. Especially for the issuance of a Root Certification Authority or for a subordinate Authority which is not under the control of the operator of the Root CA, the process is witnessed by an external Auditor or the CA Key Pair generation process is recorded and submitted to an external auditor who issues an appropriate opinion report.

6.1.1.2. Subscriber Key Pair Generation

SSL.com SHALL reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in §6.1.5 and/or §6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. SSL.com is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. SSL.com has previously been notified that the Applicant's Private Key has suffered a Key Compromise using the SSL.com's procedure for revocation request as described in §4.9.3 and §4.9.12;

5. The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the following precautions SHALL be implemented:
    a. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), SSL.com SHALL reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of §6.1.5, with the exception of RSA key sizes greater than 8192 bits, SSL.com SHALL reject Debian weak keys.
    b. In the case of ROCA vulnerability, SSL.com SHALL reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
    c. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), SSL.com SHALL reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

If the Subscriber Certificate will contain an extKeyUsage extension containing either the values id-kp-serverAuth RFC 5280 or anyExtendedKeyUsage RFC 5280, SSL.com SHALL NOT generate a Key Pair on behalf of a Subscriber, and SHALL NOT accept a certificate request using a Key Pair previously generated by SSL.com.

With the exception of Key Pairs associated with TLS Certificates, SSL.com MAY generate a Key Pair on behalf of a Subscriber.

Applicants requesting Document Signing, Code Signing or EV Code Signing Certificates must observe the criteria given in §6.2.7.4 regarding Key Pair generation and protection.

6.1.2. Private Key Delivery to Subscriber

In case SSL.com generates a Key Pair on behalf of a Subscriber, the Private Key shall be provided to the Subscriber via a secure method. Private Keys may be delivered electronically (such as through secure email or storage in a secure cloud-based system) or in a hardware cryptographic module meeting the hardware requirements described in §6.2.1.

SSL.com MAY generate and manage a Key Pair on behalf of a Subscriber as documented in §6.1.1.2.

A Key Pair associated with a Mark Certificate is unused, and there are no requirements around the generation, storage, and protection of such key pairs. In particular, SSL.com MAY generate such key pairs on behalf of Subscribers and MCs need not be revoked if the unused key pair is compromised.

In all cases of Private Key delivery:

- SSL.com shall not retain access to the Subscriber's Private Key after delivery;
- SSL.com shall protect the Private Key from activation, compromise, or modification during the delivery process;
- The Subscriber must acknowledge receipt of the Private Key(s), and

- SSL.com must deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:
    1. For hardware modules, SSL.com maintaining accountability for the location and state of the module until the Subscriber accepts possession of it and
    2. For electronic delivery of Private Keys, SSL.com encrypting key material using a cryptographic algorithm and key size at least as strong as the Private Key.

SSL.com shall deliver activation data to the Subscriber using a separate secure channel.

SSL.com shall maintain a record of the Subscriber's acknowledgement of receipt of the device containing the Subscriber's Key Pair.

If a Signing Service is generating a Private Key on behalf of the Subscriber, that Private Key SHALL NOT be transported to the Subscriber.

SSL.com or Signing Service SHALL NOT transfer Subscriber Private Keys from a cryptographic module to a Subscriber.

6.1.3 Public key delivery to certificate issuer

Public key delivery to SSL.com must be by methods conforming to §3.2.1.

6.1.4 CA Public Key delivery to Relying Parties

SSL.com shall deliver Public Keys to Relying Parties in a secure manner that helps prevent opportunities for substitution attacks.

Third parties supporting SSL.com Certificates (including but not limited to Application Software Suppliers, commercial browsers, and operating system trust stores), Subscribers and Relying Parties are permitted to use and redistribute any current, issued SSL.com Root Certificate. These are published and maintained in the SSL.com repository.

6.1.5 Key sizes

Certificates must meet the following requirements for algorithm type and key size.

(1) Root CA Certificates

Algorithm	Values
Digest algorithm	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521

(2) Subordinate CA Certificates[1]

Algorithm	Values
Digest algorithm	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521

(3) Subscriber Certificates[2]

Algorithm	Values
Digest algorithm	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521

All RSA key pairs shall have a modulus size, in bits, evenly divisible by 8.

Additional SMIME Key Sizes

For EdDSA key pairs, SSL.com SHALL:

- Ensure that the key represents a valid point on the curve25519 or curve448 elliptic curve.

For ML-DSA key pairs, SSL.com SHALL:

- Ensure the Key uses one of the following parameter sets:
  - ML-DSA-44 (OID: 2.16.840.1.101.3.4.3.17), or
  - ML-DSA-65 (OID: 2.16.840.1.101.3.4.3.18), or
  - ML-DSA-87 (OID: 2.16.840.1.101.3.4.3.19).

For ML-KEM key pairs, SSL.com SHALL:

- Ensure the Key uses one of the following parameter sets:
  - ML-KEM-512 (OID: 2.16.840.1.101.3.4.4.1), or
  - ML-KEM-768 (OID: 2.16.840.1.101.3.4.4.2), or
  - ML-KEM-1024 (OID: 2.16.840.1.101.3.4.4.3).

[1] Timestamp and Code Signing Certificates must chain up to a 4096-bit RSA or ECC equivalent (P-384) Root CA. **Effective 2021-06-01**, Subordinate CAs issuing Code Signing Certificates, Timestamp and Code Signing Certificates SHALL use a minimum RSA modulus size of 3072 bits.

[2] Timestamp and Code Signing Certificates must chain up to a 4096-bit RSA or ECC equivalent (P-384) Root CA. **Effective 2021-06-01**, Subordinate CAs issuing Code Signing Certificates, Timestamp and Code Signing Certificates SHALL use a minimum RSA modulus size of 3072 bits.

6.1.6 Public key parameters generation and quality checking

RSA: SSL.com SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^16 + 1 and 2^256 - 1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

ECDSA: SSL.com SHALL confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

SSL.com generates CA Key Pairs using secure algorithms and parameters based on current research and industry standards.

SSL.com uses CA software that performs quality checks on generated keys for both RSA and ECC algorithms and also performs regular internal audits against randomly selected samples of Subscriber Certificates per §8.7.

Additional SMIME parameter generation and quality checking EdDSA No stipulation.

ML-DSA No stipulation.

ML-KEM No stipulation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

SSL.com Root CA Private Keys shall only be utilized to sign Certificates for the following purposes:

1. Self-signed Certificates to represent the Root CA itself
2. Certificates for Subordinate CAs and Cross-Certified Subordinate CA Certificates
3. Certificates for infrastructure purposes (e.g. administrative role Certificates, internal CA operational device Certificates)
4. Certificates for OCSP Response verification

6.2 Private Key Protection and Cryptographic Module Engineering Controls

SSL.com shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of CA Private Keys outside the validated system or device specified in §6.2.7 must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. SSL.com shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic module standards and controls

All CA Private Keys shall be stored in a secure Hardware Security Module in order to perform key signing operations.

SSL.com SHALL protect its CA Private Keys in a system or device that has been validated as meeting at least FIPS 140-2 level 3, FIPS 140-3 level 3, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

6.2.2 Private key (n out of m) multi-person control

SSL.com CA Private Keys (including backups) may only be activated and/or accessed by multiple persons acting in designated trusted roles (i.e., “n-of-m multi-person control”) and using multi-factor authentication methods.

6.2.3 Private key escrow

No stipulation

6.2.4 Private key backup

SSL.com CA Private Keys are backed up via a secure and verifiable process by multiple persons acting in designated trusted roles.

Backup copies of SSL.com CA Private Keys are securely maintained. The backup copy of any CA Private Keys is encrypted and the procedures referenced in §5.1.6 must be followed regarding media storage. Only authorized personnel are allowed access to any backup copy of any CA Private Key.

Private key backup for Subscriber Certificates (if such an action is technically feasible) is exclusively under the control of the Subscriber.

Backup keys of SSL.com CA Private Keys shall only exist in encrypted form and shall never exist as plain text outside of a cryptographic module (see §6.2.1).

All copies of the CA Private Keys, including signing keys, are put beyond use at the end of their life cycle.

6.2.5 Private key archival

Subordinate CA private keys shall not be archived by third parties.

6.2.6 Private key transfer into or from a cryptographic module

Transfer of any SSL.com CA Private Keys into or from any hardware security module shall follow a secure and verifiable process conducted by multiple persons acting in designated trusted roles.

Transferred SSL.com CA Private Keys shall only exist in encrypted form and shall never exist as plain text outside of a cryptographic module (see §6.2.1).

6.2.7 Private key storage on cryptographic module

6.2.7.1 Private key storage for CA keys

SSL.com creates, stores and utilizes CA Private Keys within a secure Hardware Security Module as described in §6.2.1. Root Private Keys are stored offline in cryptographic modules or backup tokens.

6.2.7.2 Private key storage for Timestamp Authorities

Effective April 15, 2025, a Timestamp Authority MUST generate and protect Private Keys associated with its Root CA certificates and new Subordinate CA certificates with a validity period of greater than 72 months containing the `id-kp-timeStamping` KeyPurposeId in the `extKeyUsage` extension (per §7.1.2.2 g), in a Hardware Crypto Module conforming to the requirements specified in §6.2.7.1, maintained in a High Security Zone and in an offline state or air-gapped from all other networks.

Timestamp Certificates issued on or after April 15, 2025, issued by a Timestamp Authority Subordinate CA with a validity period greater than 72 months, MUST be signed by a Private Key generated and protected in a Hardware Crypto Module conforming to the requirements specified in §6.2.7.1, maintained in a High Security Zone and in an offline state or air-gapped from all other networks.

6.2.7.3 Private key storage for Signing Services

The Signing Service MUST ensure that a Subscriber's Private Key is generated, stored, and used in a secure environment that has controls to prevent theft or misuse. A Signing Service MUST enforce multi-factor authentication or server-to-server authentication to access and authorize Code Signing.

For Code Signing Certificates, Signing Services SHALL protect Subscriber Private Keys in a Hardware Crypto Module conforming to at least FIPS 140-2 level 2 or Common Criteria EAL 4+.

Techniques that MUST be used to satisfy this requirement include:

1. Use of an Hardware Crypto Module, verified by means of a FIPS or Common Criteria certificate; or
2. A cloud-based key generation and protection solution with the following requirements:
    a. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements;
    b. Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.
3. A Hardware Crypto Module provided by SSL.com;

4. Contractual terms in the Subscriber Agreement requiring the Subscriber to protect the Private Key to a standard of at least FIPS 140-2 level 2 or Common Criteria EAL 4+ and with compliance being confirmed by means of an audit.

6.2.7.4 Subscriber Private Key protection and verification

6.2.7.4.1 Subscriber Private Key protection

For Non-EV Code Signing Certificates issued prior to June 1, 2023, SSL.com MUST obtain a representation from the Subscriber that the Subscriber will use one of the following options to generate and protect their Code Signing Certificate Private Keys:

1. A Trusted Platform Module (TPM) that generates and secures a Key Pair and that can document the Subscriber's Private Key protection through a TPM key attestation.
2. A suitable Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2, Common Criteria EAL 4+, or equivalent.
3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140-2 Level 2 or Common Criteria EAL 4+). The Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

For Non-EV Code Signing Certificates issued prior to June 1, 2023, SSL.com MUST recommend that the Subscriber protect Private Keys using the method described in §6.2.7.4.1(1) or 6.2.7.4.1(2) over the method described in §6.2.7.4.1(3) and obligate the Subscriber to protect Private Keys in accordance with §9.6.3 (2).

For EV Code Signing Certificates issued prior to June 1, 2023, SSL.com SHALL ensure that the Subscriber's Private Key is generated, stored and used in a Hardware Crypto Module that meets or exceeds the requirements of FIPS 140-2 level 2 or Common Criteria EAL 4+. Acceptable methods of satisfying this requirement include (but are not limited to) the following:

1. SSL.com ships a suitable Hardware Crypto Module, with a preinstalled Private Key, in the form of a smartcard or USB device or similar;
2. The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate indicating that the Private Key is managed in a suitable Hardware Crypto Module;
3. The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 2.

Effective 2023-06-01, Subscriber Private Keys for Code Signing Certificates SHALL be protected per the following requirements. SSL.com MUST obtain a contractual representation from the Subscriber that the Subscriber will use one of the following options to generate and protect their Code Signing Certificate Private Keys in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+:

1. Subscriber uses a Hardware Crypto Module meeting the specified requirement;

2. Subscriber uses a cloud-base key generation and protection solution with the following requirements:
    a. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements;
    b. Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.
3. Subscriber uses a Signing Service which meets the requirements of §6.2.7.3.

For Document Signing Certificate Subscribers, SSL.com shall ensure that the Subscriber's Private Key is generated:

1. either by using a trustworthy system, taking all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key, and then securely transferred in a Hardware Crypto Module that meets or exceeds the requirements of FIPS 140-2 level 2 or Common Criteria EAL 4+;
2. directly generated by and stored in such a secure cryptographic hardware device; or
3. be stored in a Hardware Crypto Module that meets or exceeds the requirements of FIPS 140-2 level 2 or Common Criteria EAL 4+.

All key pairs associated with Document Signing Certificates must be stored in a secure cryptographic hardware device that:

- is certified by:
    - FIPS 140-2 Level 2; or
    - Common Criteria (ISO 15408 & ISO 18045) - Protection Profiles CEN prEN 14169 (all parts applicable to the device type) or standards such as CEN EN 419 241 series or equivalent, for remotely managed devices; or
    - an EU Member State as a Qualified Signature Creation Device (QSCD) after 1 July 2016, or that was recognized as a Secure Signature Creation Device (SSCD) by an EU Member State designated body before 1 July 2016.
- is controlled by the signer (or by the subscriber if the signer is not a Natural Person):
    - either directly, by possession (after secure hand-over to the subscriber when applicable). In this case:
        - the activation of the private key must require the signer's authentication and
        - the device must prevent exportation or duplication of the private key.
    - or via a third party managing the secure cryptographic hardware device on behalf of the signer. In this case:
        - the key activation must rely on at least a 2-factor authentication (2FA) process, except from cases in which more flexibility is desirable; for

example, in automated e-signing / e-sealing scenarios or when the Subscriber acknowledges and accepts the associated risks, and
- no duplication of the private key is allowed, except for duly documented service availability purpose, and the duplicated key must abide at least the same security measures as the original;

Special controls are in place to ensure that any cryptographic hardware used has not been tampered with and is functioning correctly. The integrity of the hardware and software used for key generation, and of any interfaces used to access the hardware and software, is tested before production usage.

6.2.7.4.2 Subscriber Private Key verification

Effective 2023-06-01, for Code Signing Certificates, SSL.com SHALL ensure that the Subscriber's Private Key is generated, stored, and used in a suitable Hardware Crypto Module that meets or exceeds the requirements specified in §6.2.7.4.1. One of the following methods MUST be employed to satisfy this requirement:

1. SSL.com ships a suitable Hardware Crypto Module, with one or more pre-generated Key Pairs that SSL.com has generated using the Hardware Crypto Module;
2. The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate, commonly known as key attestation, indicating that the Private Key was generated in a non-exportable way using a suitable Hardware Crypto Module;
3. The Subscriber uses a prescribed crypto library by SSL.com and a suitable Hardware Crypto Module combination for the Key Pair generation and storage;
4. The Subscriber provides an internal or external IT audit indicating that it is only using a suitable Hardware Crypto Module to generate Key Pairs to be associated with Code Signing Certificates;
5. The Subscriber provides a suitable report from the cloud-based key protection solution subscription and resources configuration protecting the Private Key in a suitable Hardware Crypto Module;
6. SSL.com relies on a report provided by the Applicant that is signed by an auditor who is approved by SSL.com and who has IT and security training or is a CISA, who witnessed the Key Pair creation in a suitable Hardware Crypto Module solution including a cloud-based key generation and protection solution;
7. The Subscriber provides an agreement that they use a Signing Service meeting the requirements of §6.2.7.3.

6.2.8 Method of activating Private Key

SSL.com activates CA Private Keys using only methods which observe the instructions and specifications of the manufacturer of the relevant cryptographic module and via a secure and verifiable process, conducted by multiple persons acting in designated trusted roles and using multi-factor authentication.

Applicants and Subscribers are instructed to protect their Private Keys using the standards described in the appropriate Subscriber Agreement. Subscribers are solely responsible for protecting their Private Keys.

6.2.9 Method of deactivating Private Key

SSL.com CA Private Keys maintained in any cryptographic hardware shall be deactivated when not in use, using documented procedures which ensure that appropriate physical and logical security controls are observed.

6.2.10 Method of destroying Private Key

CA Private Keys shall be destroyed when they are no longer needed. As part of the process of destruction of a CA Private Key:

- Any CA Private Key stored in any Hardware Security Module (HSM) is destroyed using the secure deletion function of the HSM, per the manufacturer's instructions. Only the physical instance of the CA Private Key stored in the HSM under consideration will be destroyed.
- Any other encrypted copies and fragments of the CA Private Key shall be destroyed over a reasonable amount of time.

If a CA cryptographic device is being permanently removed from service, then any CA Private Key contained within the device used for any cryptographic purpose is erased from the device. If a CA cryptographic device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed.

The destruction of any CA Private Key and/or CA cryptographic device shall only be performed by appropriate personnel acting in trusted roles and documented using verifiable methods.

Subscribers are solely responsible for the complete and secure destruction of all copies and fragments of the Subscriber's Private Key at the end of the Key Pair life cycle.

6.2.11 Cryptographic Module Rating

See §6.2.1

6.3 Other aspects of Key Pair management

6.3.1 Public key archival

SSL.com archives Public Keys as described in §5.5.

6.3.2 Certificate operational periods and Key Pair usage periods

The maximum validity period of CA Certificates is:

- **Twenty-five (25) years** for Root CAs,

- **Fifteen (15) years** for Intermediate CAs.

The maximum validity period of end-entity non-TLS Certificates is:

- **One hundred and thirty-five (135) months** for Timestamp or EV Timestamp Authorities
- **Sixty (60) months** for Subscriber Client Authentication Certificates
- **Eight hundred and twenty (820) days** for S/MIME Subscriber Certificates
- **Twenty-four (24) months** for NAESB compliant Certificates
- **Thirty-nine (39) months** for Document Signing Certificates
- **Three hundred and ninety-eight (398) days** for Mark Certificates

The maximum validity period of end-entity TLS Certificates is defined in the following table:

Reference for maximum Validity Periods of Subscriber TLS Certificates (EV and non-EV)

Certificate issued on or after	Certificate issued before	Maximum Validity Period
	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days
March 15, 2027	March 15, 2029	100 days
March 15, 2029		47 days

The maximum validity period of Code Signing Certificates is defined in the following table:

Reference for maximum Validity Periods of Code Signing Subscriber Certificates (EV and non-EV)

Certificate issued on or after	Certificate issued before	Maximum Validity Period
	March 1, 2026	39 months
March 1, 2026		460 days

If an Applicant is a licensee of a Registered Mark or Word Mark rather than the Registrant, the expiration date of the Mark Certificate SHALL have an expiration date that is no later than the final expiration date of the license held by the Applicant to use the Registered Mark or Word Mark, which SHALL be confirmed by SSL.com during the verification process.

The operational period must be defined according to the size of the keys and the current technological developments at the field of cryptography to guarantee the best level of security and efficiency of use.

Subscribers should not reuse Key Pairs when requesting new certificates.

The Timestamp Certificate Key Pair MUST meet the requirements in §6.1.5. SSL.com or Timestamp Authority SHALL NOT use a Private Key associated with a Timestamp Certificate more than 15 months after the `notBefore` date of a Timestamp Certificate.

Effective April 15, 2025, Private Keys associated with Timestamp Certificates issued for greater than 15 months MUST be removed from the Hardware Crypto Module protecting the Private

Key within 18 months after issuance of the Timestamp Certificate. For Timestamp Certificates issued on or after June 1, 2024, SSL.com SHALL log the removal of the Private Key from the Hardware Crypto Module through means of a key deletion ceremony performed by the CA and witnessed and signed-off by at least two Trusted Role members. SSL.com MAY also perform a key destruction ceremony, meaning that all copies of that private key are unequivocally/securely destroyed (i.e. without a way to recover the key), including any instance of the key as part of a backup, to satisfy this requirement.

SSL.com MAY maintain existing backup sets containing the Private Key corresponding to a Timestamp Certificate. SSL.com SHOULD NOT restore the Private Key corresponding to a Timestamp Certificate contained within the backup if the Timestamp Certificate was issued more than 15 months prior to restoration of the backup. If SSL.com does restore such a Private Key, SSL.com SHALL only restore the Private Key in a suitable HSM while it's maintained in a High Security Zone and in an offline state or air-gapped from all other networks and perform a new key destruction ceremony prior to the HSM being brought to an online state.

6.4 Activation data

SSL.com shall protect and secure any data used to activate any CA Private Key utilized in the SSL.com PKI, including any PIN, passphrase, or portion of a Private Key used in a key-splitting scheme. See also §6.2.8.

6.4.1 Activation Data Generation and Installation

SSL.com shall activate and install SSL.com CA Private Keys into any cryptographic module using only methods which observe the instructions and specifications of the manufacturer of the relevant cryptographic module. Initial generation, activation and installation shall be via a CA key ceremony as described in §6.1.1.1.

Separately generated and secured Activation Data is used to protect access to Private Keys in cases where SSL.com generates Key Pairs for Subscribers.

6.4.2 Activation data protection

SSL.com shall protect activation data from compromise or disclosure. Appropriate cryptographic and physical access controls shall be implemented to prevent unauthorized use of any CA Private Key activation data.

In cases where SSL.com generates Key Pairs for Subscribers, SSL.com shall only provide Activation Data via a secure channel which is separate from delivery of the cryptographic module containing the related Private Key.

6.4.3 Other aspects of activation data

All activation data related to SSL.com CA Private Keys and associated root Certificates is held only by SSL.com personnel holding clearly defined trusted roles.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All systems used as part of the SSL.com PKI (including CA servers, support and vetting workstations, and systems utilized by trusted third parties) are:

- Configured, maintained and secured using industry best practices
- Operated on trustworthy software
- Regularly scanned for malicious code and protected against spyware and viruses
- Updated with recommended security patches within six months of the security patch's availability, unless documented testing determines that the security patch would introduce additional vulnerabilities

All systems are configured to:

- Authenticate the identity of users before permitting access to the system or applications
- Manage the privileges of users and limit users to their assigned roles
- Generate and archive audit records for all transactions
- Enforce domain integrity boundaries for security critical processes, and
- Support recovery from key or system failure.

Where practicable, SSL.com shall implement multi-factor authentication to each PKI component that supports multi-factor authentication, including accounts 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

SSL.com CA's system development controls include (but are not limited to) the following:

- All software used for CA systems follows a documented development process prior to implementation
- All components of the CA system, including all hardware and software, are obtained in a manner that reduces the probability that hardware or software has been falsified, modified or tampered with in any way
- All hardware used in CA systems shall be shipped and/or delivered using secure packing methodology (including tamperproof packaging where appropriate) along with complete tracking records

- The hardware and software used for CA systems are specifically used to performing CA activities, and only software, hardware or network connections directly required for CA operations are installed or permitted
- All hardware and software updates to CA systems are documented, and are securely purchased, developed, and/or installed only by personnel holding a Trusted role.

Regarding Linting software:

- SSL.com SHOULD monitor for updated versions of any third party Linting software utilized in the CA service, and plan for updates no later than three (3) months from the release of the update.
- SSL.com MAY perform Linting on the corpus of its unexpired, un-revoked Subscriber Certificates whenever it updates the Linting software.

6.6.2 Security management controls

SSL.com incorporates system-wide security controls and monitoring to CA software configurations. A documented process is used to authenticate modification, installation, and management of software utilized in or interacting with CA systems.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

SSL.com maintains network security controls to protect all operations related to the SSL.com PKI.

These controls observe the standards established in the most recent version of the CAB Forum Network and Certificate System Security Requirements (https://cabforum.org/network-security-requirements/), incorporating the necessary time for implementation.

All SSL.com PKI-related systems are segmented into networks or zones based on their functional, logical, and/or physical relationship. The same security controls are applied to all systems co-located in the same zone or network. To protect data confidentiality, integrity, and availability, systems, networks and communications are protected by appropriate physical and logical controls to protect data confidentiality, integrity, and availability including (but not limited to) firewalls, filters, port blocking and any other hardware or software methods deemed appropriate.

SSL.com implements measures to protect PKI-related systems and communications within and between these zones and networks, and to also secure all communications between these zones and networks and:

- Non-PKI-related systems, networks and/or zones, including those SSL.com and/or third party systems that do not provide PKI-related services) and

- Any systems on public networks

All network boundary control devices or systems (including firewalls, switches, routers, gateways, or other devices) are configured with rules to allow only services, protocols, ports, and communications necessary for operations. All systems supporting SSL.com PKI operations (including third-party systems) are configured to use only accounts, applications, services, protocols, and ports approved by SSL.com.

Physical access to hardware utilized for SSL.com CA Private Keys, including cryptographic modules and related devices, is secured within a facility which meets the approval of Qualified Auditors (see §5.1.2).

Administrator (or higher) access to systems is only granted to a person acting in an accountable Trusted Role (per §5.2.1) and any such access is logged (see §5.4.1).

SSL.com continually reviews system configurations to detect and correct departures from these security controls.

SSL.com performs vulnerability assessments according to §5.4.8. Any vulnerabilities found are triaged and remediated according to the their severity as follows: - Critical severity vulnerabilities are addressed within 96 hours - High severity vulnerabilities are addressed within 10 days - Medium or lower severity vulnerabilities are addressed within 3 months, where feasible.

Any exceptions are granted by the information security and compliance units only upon documented justification, based on the risk, and considering the environmental / temporal parameters and any complementary controls.

6.8 Time-stamping

SSL.com operates a Timestamp Authority that complies with RFC 3161 and recommends to Subscribers that they use the SSL.com's Timestamp Authority to timestamp signed code.

SSL.com ensures that the accuracy of time sources used in all time-stamping operations are properly maintained, trusted and verifiable via NTP (Network Time Protocol). SSL.com incorporates a manual and digital process which work in tandem to ensure authenticity of system time. More information is also available in §5.5.5.

SSL.com ensures that clock synchronization is maintained when a leap second occurs. SSL.com synchronizes its timestamp server at least every 24 hours with a UTC(k) time source. The timestamp server automatically detects and reports on clock drifts or jumps out of synchronization with UTC. Clock adjustments of one second or greater are auditable events. Any changes to the signing process are an auditable event.

SSL.com SHALL reject timestamp requests containing a `MessageImprint` calculated using the SHA-1 digest algorithm.

The digest algorithm used to sign Timestamp tokens must match the digest algorithm used to sign the Timestamp Certificate.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profiles

SSL.com shall meet the technical requirements set forth in §6.1.5 and §6.1.6 of the SSL.com CP/CPS.

SSL.com shall generate Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1 Version Numbers

The SSL.com PKI issues Certificates in compliance with the X.509 Version 3, which corresponds to certificate version number 2.

7.1.2 Certificate Content and Extensions

SSL.com Certificates comply with RFC 5280 and with applicable best industry practices.

A tabled view of the most common certificate profiles used by SSL.com are listed in Annex A (SSL.com Certificate Profiles).

7.1.2.1 Root CA Certificate

a. basicConstraints

- This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

b. keyUsage

- This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

c. certificatePolicies

- This extension SHOULD NOT be present.

d. extKeyUsage

- This extension MUST NOT be present.

7.1.2.2 Subordinate CA Certificate

a. certificatePolicies

- This extension must be present and should not be marked critical.
    - certificatePolicies:policyIdentifier (Required): See §7.1.6
- The following fields may be present if the Subordinate CA is not an Affiliate of SSL.com.
    - certificatePolicies:policyQualifiers:policyQualifierId (Optional)

        - id-qt 1 RFC 5280
        - certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)
- HTTP URL for the Root CA's Certificate Policy, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by SSL.com and the Subordinate CA.

b. cRLDistributionPoints (if applicable)

- This extension must be present and must not be marked critical. It must contain the HTTP URL of the Issuing CA's CRL service.

c. authorityInformationAccess (if applicable)

- If the Issuing CA issues Code Signing or Time-stamping Certificates, this extension MUST be present and MUST NOT be marked critical. The extension MUST contain the HTTP URL of the Issuing CA's certificate (accessMethod = `1.3.6.1.5.5.7.48.2`) and if the CA provides OCSP responses, the HTTP URL for the CA's OCSP responder (accessMethod = `1.3.6.1.5.5.7.48.1`).

- For all other Issuing CAs this extension SHOULD be present. It MUST NOT be marked critical. It SHOULD contain the HTTP URL of the Issuing CA's certificate (accessMethod = `1.3.6.1.5.5.7.48.2`) and it MAY contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = `1.3.6.1.5.5.7.48.1`).

d. basicConstraints (critical)

- The cA field is set true. The pathLenConstraint field may be present.

e. keyUsage (critical)

- keyCertSign and cRLSign bits are set. Optionally, digitalSignature can be set.

f. nameConstraints (optional)

- If present, this extension should not be marked critical[3].

g. extkeyUsage

- For Cross Certificates that share a Subject Distinguished Name and Subject Public Key with a Root Certificate operated in accordance with this CP/CPS, this extension MAY be present. If present, this extension SHOULD NOT be marked critical. This extension MUST only contain usages for which the issuing CA has verified the Cross Certificate is authorized to assert. This extension MAY contain the `anyExtendedKeyUsage` RFC 5280 usage, if the Root Certificate(s) associated with this Cross Certificate are operated by the same organization as the issuing Root Certificate.

- For all other Subordinate CA Certificates, including Technically Constrained Subordinate CA Certificates:

[3] Non-critical Name Constraints are an exception to RFC 5280 (4.2.1.10), however, they may be used until the Name Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.

- This extension MUST be present and SHOULD NOT be marked critical.
- For Subordinate CA Certificates that will be used to issue TLS certificates, the value `id-kp-serverAuth` RFC 5280 MUST be present. The value `id-kp-clientAuth` RFC 5280 MAY be present. The values `id-kp-emailProtection` RFC 5280, `id-kp-codeSigning` RFC 5280, `id-kp-timeStamping` RFC 5280, and `anyExtendedKeyUsage` RFC 5280 MUST NOT be present. Other values SHOULD NOT be present.
- For Subordinate CA Certificates that are not used to issue TLS certificates, then the value `id-kp-serverAuth` RFC 5280 MUST NOT be present. Other values MAY be present, but SHOULD NOT combine multiple independent key purposes (e.g. including `id-kp-timeStamping` RFC 5280 with `id-kp-codeSigning` RFC 5280).
- For Subordinate CA Certificates that will be used to issue Mark Certificates, value MUST contain `id-kp-BrandIndicatorforMessageIdentification` (OID: `1.3.6.1.5.5.7.3.31`) as specified in Section 7 of the IETF Internet-Draft at https://tools.ietf.org/html/draft-chuang-bimi-certificate-00. This indicates the application of the Mark Certificate Profile. Other KeyPurposeIds MUST NOT be included.

h. authorityKeyIdentifier (required)

- This extension MUST be present and MUST NOT be marked critical. It MUST contain a keyIdentifier field and it MUST NOT contain a authorityCertIssuer or authorityCertSerialNumber field.

- By issuing a Subordinate CA Certificate, SSL.com represents that it followed the procedure set forth in this CP/CPS to verify that, as of the CA Certificate's issuance date, all of the Subject Information was validated and found to be accurate.

The following provisions SHALL apply with regards to the issuance of end entity S/MIME Certificates by Extant S/MIME CAs:

1. Following the Effective Date for v1.0.0 of S/MIME Baseline Requirements (September 1, 2023) an Extant S/MIME CA MAY continue to issue end entity S/MIME Certificates that are compliant with these Requirements.
2. On or after September 15, 2024, all newly-issued Publicly-Trusted end entity S/MIME Certificates SHALL be issued from S/MIME Subordinate CAs that are compliant with these Requirements.
3. For backwards compatibility, Extant S/MIME CA Certificates that share the same Public Keys with S/MIME Subordinate CAs that are compliant with these Requirements, or are no longer used for signing end entity S/MIME Certificates, are not required to be revoked.

7.1.2.3 Subscriber Certificate

a. certificatePolicies

- This extension must be present and should not be marked critical.

- certificatePolicies:policyIdentifier (Required): (See §7.1.6)
- The following extensions may be present:
  - certificatePolicies:policyQualifiers:policyQualifierId (Recommended)
    - id-qt 1 RFC 5280
  - certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)
    - HTTP URL for the Subordinate CA's Certificate Policyies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by SSL.com and the Subordinate CA.

b. cRLDistributionPoints (if applicable)

- The CRL Distribution Points extension MUST be present in TLS Subscriber Certificates that
  1. do not qualify as "Short-lived Subscriber Certificates" and
  2. do not include an Authority Information Access extension with an id-ad-ocsp accessMethod.
- The CRL Distribution Points extension is OPTIONAL in Short-lived TLS Subscriber Certificates.
- When present, the CRL Distribution Points extension MUST contain at least one `DistributionPoint`; containing more than one is NOT RECOMMENDED. All `DistributionPoint` items must be formatted as follows:

Field	Presence	Description
`distributionPoint`	MUST	The `DistributionPointName` MUST be a `fullName` formatted as described below.
`reasons`	MUST NOT	
`cRLIssuer`	MUST NOT	

A `fullName` MUST contain at least one `GeneralName`; it MAY contain more than one. All `GeneralNames` MUST be of type `uniformResourceIdentifier`, and the scheme of each MUST be "http". The first `GeneralName` must contain the HTTP URL of the Issuing CA's CRL service for this certificate.

c. authorityInformationAccess (if applicable)

- For TLS, Code Signing and Time-stamping Certificates this extension MUST be present and for other types of Certificates it MAY be present. If present, it MUST NOT be marked critical. For TLS Certificates it MUST contain the HTTP URL of the Issuing CA's OCSP responder (`accessMethod` = `1.3.6.1.5.5.7.48.1`) and SHOULD contain the HTTP URL of the Issuing CA's certificate (`accessMethod` = `1.3.6.1.5.5.7.48.2`). For Code Signing or Timestamping Certificates, it MUST contain the HTTP URL of the Issuing CA's certificate (`accessMethod` = `1.3.6.1.5.5.7.48.2`) and if the CA provides OCSP responses, the HTTP URL for the CA's OCSP responder (accessMethod = `1.3.6.1.5.5.7.48.1`). For all other Subscriber Certificates, it MAY contain the HTTP URL of the Issuing CA's certificate (`accessMethod` = `1.3.6.1.5.5.7.48.2`) and if the CA

provides OCSP responses, the HTTP URL for the CA's OCSP responder (accessMethod = `1.3.6.1.5.5.7.48.1`).

d. basicConstraints (optional)

- This extension should not be present. If present, the cA field must be set false.

e. keyUsage (optional)

- If present, bit positions for keyCertSign and cRLSign must not be set.

f. extKeyUsage (required)

- Depending on the usage of the certificate, the proper extended key usage (EKU) will be applied. More information available in Annex A.
- For Timestamp Certificates, this extention MUST be marked critical. For other types, the extention SHOULD NOT be marked critical.
- For TLS Certificates either the value `id-kp-serverAuth` RFC 5280 or `id-kp-clientAuth` RFC 5280 or both values MUST be present. `id-kp-emailProtection` RFC 5280 MAY be present. Other values SHOULD NOT be present. The value `anyExtendedKeyUsage` MUST NOT be present.
- For Code Signing Certificates the value `id-kp-codeSigning` RFC 5280 MUST be present. The value `lifetimeSigning` (`1.3.6.1.4.1.311.10.3.13`) MAY be present. The value `anyExtendedKeyUsage` (2.5.29.37.0), `serverAuth` (`1.3.6.1.5.5.7.3.1`), `emailProtection` (`1.3.6.1.5.5.7.3.4`) and `timeStamping` (`1.3.6.1.5.5.7.3.8`) MUST NOT be present. Other values SHOULD NOT be present. If any other value is present, SSL.com MUST have a business agreement with a Platform vendor requiring that EKU in order to issue a Platform-specific code signing certificate with that EKU.
- For Timestamp Certificates the value `id-kp-timeStamping` RFC 5280 MUST be present. The value `anyExtendedKeyUsage` (2.5.29.37.0), `serverAuth` (`1.3.6.1.5.5.7.3.1`), `emailProtection` (`1.3.6.1.5.5.7.3.4`) and `codeSigning` RFC 5280 MUST NOT be present. Other values SHOULD NOT be present. If any other value is present, SSL.com MUST have a business agreement with a Platform vendor requiring that EKU in order to issue a Platform-specific code signing certificate with that EKU.
- For Mark Certificates the value `id-kp-BrandIndicatorforMessageIdentification` (OID: `1.3.6.1.5.5.7.3.31`) as specified in Section 7 of the IETF Internet-Draft at https://tools.ietf.org/html/draft-chuang-bimi-certificate-00 MUST be present. Other KeyPurposeIds MUST NOT be included.
- It is forbidden for Intermediate CAs to issue end-entity Certificates which blend the serverAuth (`1.3.6.1.5.5.7.3.1`), emailProtection (`1.3.6.1.5.5.7.3.2`) and codeSigning (`1.3.6.1.5.5.7.3.3`) extended key usages.

g. DelegationUsage (optional)

- For TLS Certificates, SSL.com supports the IETF draft https://datatracker.ietf.org/doc/html/draft-ietf-tls-subcerts for Delegated Credentials.

h. signedCertificateTimestampList (OID: 1.3.6.1.4.1.11129.2.4.2)

- This extension MUST NOT be critical

- For Mark Certificates, this extension MUST be present. Mark precertificates MUST be logged to at least one of well-known Certificate Transparency (CT) logs RFC 6962 which then provide Signed Certificate Timestamps (SCT). The SCT must be added to the Certificate Transparency extension as a SignedCertificateTimestampList encoded as an octet string RFC 6962 section 3.3.

i. logotype extension (OID: 1.3.6.1.5.5.7.1.12)

- This extension SHOULD NOT be marked critical.
- For Mark Certificates this extension MUST be present.
- Ths extension MUST:
    1. contain subjectLogo with a LogotypeData element RFC 3709 containing the Mark Representation asserted by the Subject of the Mark Certificate and verified by SSL.com.
    2. embed the image element in "data:" URL as defined in RFC6170 section 4.
- The Mark Representation MUST:
    1. be embedded a secured SVG image RFC 6170
    2. use the SVG Tiny PS profile to secure the SVG
    3. be compressed
    4. follow other requirements set forth in RFC 6170 section 5.2
- The Mark Representation MUST NOT contain `<script>` tags. Additionally the AuthIndicators Working Group has published a SVG Tiny PS Guidelines document as well as a RNC tool to help validate the SVG. The MC SVG is also required to follow those specifications.
- SSL.com SHALL verify that the Applicant provided Mark Representation meets this secure profile.

7.1.2.4 OCSP Responder Certificate

a. certificatePolicies

- **Effective 2023-09-15**, for OCSP Responder Certificates issuing responses for TLS Certificates, this extension MUST NOT be present.

b. cRLDistributionPoints

- **Effective 2023-09-15**, for OCSP Responder Certificates issuing responses for TLS Certificates, this extension MUST NOT be present.

c. authorityInformationAccess

- For OCSP Responder certificates issuing responses for TLS Certificates, this extension is NOT RECOMMENDED, as the Relying Party should already possess the necessary information. In order to validate the given Responder certificate, the Relying Party must have access to the Issuing CA's certificate, eliminating the need to provide `id-ad-caIssuers`. Similarly, because of the requirement for an OCSP Responder certificate to include the `id-pkix-ocsp-nocheck` extension, it is not necessary to provide `id-ad-ocsp`, as such responses will not be checked by Relying Parties.

- If present, for OCSP Responder certificates issuing responses for TLS Certificates the `AuthorityInfoAccessSyntax` MUST contain one or more `AccessDescriptions`. Each `AccessDescription` MUST only contain a permitted `accessMethod`, as detailed below, and each `AuthorityInfoAccessSyntax` MUST contain all required `AccessDescriptions`.

Access Method	OID	Access Location	Presence	Maximum	Description
`id-ad-ocsp`	`1.3.6.1.5.5.7.48.1`	`uniformResourceIdentifier`	NOT RECOMMENDED	*	A HTTP URL of the Issuing CA's OCSP responder.
Any other value	-	-	MUST NOT	-	No other `accessMethods` may be used.

d. basicConstraints (optional)

- OCSP Responder certificates MUST NOT be CA certificates. The issuing CA may indicate this one of two ways: by omission of the `basicConstraints` extension, or through the inclusion of a `basicConstraints` extension that sets the `cA` boolean to FALSE.

Field	Description
`cA`	MUST be FALSE
`pathLenConstraint`	MUST NOT be present

Note: Due to DER encoding rules regarding the encoding of DEFAULT values within OPTIONAL fields, a `basicConstraints` extension that sets the `cA` boolean to FALSE MUST have an `extnValue OCTET STRING` which is exactly the hex-encoded bytes `3000`, the encoded representation of an empty ASN.1 `SEQUENCE` value.

e. keyUsage (required)

Key Usage	Permitted	Required
`digitalSignature`	Y	Y
`nonRepudiation`	N	–
`keyEncipherment`	N	–
`dataEncipherment`	N	–
`keyAgreement`	N	–
`keyCertSign`	N	–
`cRLSign`	N	–
`encipherOnly`	N	–
`decipherOnly`	N	–

f. extKeyUsage (required)

Key Purpose	OID	Presence
`id-kp-OCSPSigning`	`1.3.6.1.5.5.7.3.9`	MUST
Any other value	-	MUST NOT

7.1.2.5 All Certificates

All other fields and extensions must be set in accordance with RFC 5280. SSL.com shall not issue a Certificate that contains a keyUsage flag, extKeyUsage value, Certificate extension, or other data not specified in §7.1.2.1, §7.1.2.2, §7.1.2.3 and Annex A unless SSL.com is aware of a reason for including the data in the Certificate.

SSL.com shall not issue a Server TLS or S/MIME Certificate with:

1. Extensions that do not apply in the context of the public Internet (such as an extKeyUsage key purpose for a service that is only valid in the context of a privately managed network), unless:
    a. such value falls within an OID arc for which the Applicant demonstrates ownership, or
    b. the Applicant can otherwise demonstrate the right to assert the data in a public context.
    c. the extension is defined within an open standards specification and intended for use by other organizations. A Certificate that includes such an extension MUST conform to the specifications of the open standard and this CP/CPS.
2. Field or extension values which have not been validated according to the processes and procedures described in this CP/CPS.

All Certificates include the following extensions:

- Authority Key Identifier: Provides information to identify the Public Key corresponding to the Private Key used to sign a Certificate. This field contains the “Subject Key Identifier” of the issuing CA’s Certificate
- Subject Key Identifier: Identifies a particular Public Key uniquely. It contains the ID of the Certificate Holder’s key

7.1.2.6 Application of RFC 5280

For purposes of clarification, a Precertificate, as described in RFC 6962 - Certificate Transparency, shall not be considered to be a “certificate” subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

7.1.3 Algorithm object identifiers

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to the `subjectPublicKeyInfo` field within a Certificate or Precertificate. No other encodings are permitted.

7.1.3.1.1 RSA

SSL.com SHALL indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters MUST be present, and MUST be an explicit NULL.

SSL.com SHALL NOT use a different algorithm, such as the id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) algorithm identifier, to indicate an RSA key.

When encoded, the `AlgorithmIdentifier` for RSA keys MUST be byte-for-byte identical with the following hex-encoded bytes: `300d06092a864886f70d0101010500`

7.1.3.1.2 ECDSA

SSL.com SHALL indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters SHALL use the `namedCurve` encoding.

- For P-256 keys, the `namedCurve` MUST be secp256r1 (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, the `namedCurve` MUST be secp384r1 (OID: 1.3.132.0.34).
- For P-521 keys, the `namedCurve` MUST be secp521r1 (OID: 1.3.132.0.35).

When encoded, the `AlgorithmIdentifier` for ECDSA keys MUST be byte-for-byte identical with the following hex-encoded bytes:

- For P-256 keys, `301306072a8648ce3d020106082a8648ce3d030107`.
- For P-384 keys, `301006072a8648ce3d020106052b81040022`.
- For P-521 keys, `301006072a8648ce3d020106052b81040023`.

7.1.3.1.3 EdDSA

For S/MIME Certificates:

SSL.com SHALL indicate an EdDSA key using one of the following algorithm identifiers below:

- For curve25519 keys, the `algorithm` SHALL be id-Ed25519 (OID: 1.3.101.112).
- For curve448 keys, the `algorithm` SHALL be id-Ed448 (OID: 1.3.101.113).

The parameters for EdDSA keys SHALL be absent.

When encoded, the `AlgorithmIdentifier` for EdDSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For Curve25519 keys, `300506032b6570`.
- For Curve448 keys, `300506032b6571`.

7.1.3.1.4 ML-DSA

For S/MIME Certificates:

SSL.com SHALL indicate an ML-DSA key using one of the following algorithm identifiers below:

- ML-DSA-44 (OID: 2.16.840.1.101.3.4.3.17), or
- ML-DSA-65 (OID: 2.16.840.1.101.3.4.3.18), or
- ML-DSA-87 (OID: 2.16.840.1.101.3.4.3.19).

The parameters for ML-DSA keys SHALL be absent. SSL.com MUST NOT use HashML-DSA; only "pure" ML-DSA is permitted.

When encoded, the AlgorithmIdentifier for ML-DSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For ML-DSA-44, `300b0609608648016503040311`.
- For ML-DSA-65, `300b0609608648016503040312`.
- For ML-DSA-87, `300b0609608648016503040313`.

7.1.3.1.5 ML-KEM

For S/MIME Certificates:

SSL.com SHALL indicate an ML-KEM key using one of the following algorithm identifiers below:

- ML-KEM-512 (OID: 2.16.840.1.101.3.4.4.1), or
- ML-KEM-768 (OID: 2.16.840.1.101.3.4.4.2), or
- ML-KEM-1024 (OID: 2.16.840.1.101.3.4.4.3).

The parameters for ML-KEM keys SHALL be absent.

When encoded, the AlgorithmIdentifier for ML-KEM keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For ML-KEM-512, `300b0609608648016503040401`.
- For ML-KEM-768, `300b0609608648016503040402`.
- For ML-KEM-1024, `300b0609608648016503040403`.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a CA Private Key MUST conform to this CP/CPS on the use of the `AlgorithmIdentifier` or `AlgorithmIdentifier`-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The `signatureAlgorithm` field of a Certificate or Precertificate.
- The `signature` field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).

- The `signatureAlgorithm` field of a CertificateList
- The `signature` field of a TBSCertList
- The `signatureAlgorithm` field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

SSL.com SHALL use one of the following signature algorithms and encodings. When encoded, the `AlgorithmIdentifier` MUST be byte-for-byte identical with the specified hex-encoded bytes.

- RSASSA-PKCS1-v1_5 with SHA-256:

  Encoding: `300d06092a864886f70d01010b0500`.

- RSASSA-PKCS1-v1_5 with SHA-384:

  Encoding: `300d06092a864886f70d01010c0500`.

- RSASSA-PKCS1-v1_5 with SHA-512:

  Encoding: `300d06092a864886f70d01010d0500`.

- RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes:

  Encoding:

  ```
  304106092a864886f70d01010a3034a00f300d06096086480165030402 01
  0500a11c301a06092a864886f70d010108300d06096086480165030402 01
  0500a203020120
  ```

- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes:

  Encoding:

  ```
  304106092a864886f70d01010a3034a00f300d06096086480165030402 02
  0500a11c301a06092a864886f70d010108300d06096086480165030402 02
  0500a203020130
  ```

- RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:

  Encoding:

  ```
  304106092a864886f70d01010a3034a00f300d06096086480165030402 03
  0500a11c301a06092a864886f70d010108300d06096086480165030402 03
  0500a203020140
  ```

In addition, SSL.com MAY use the following signature algorithm and encoding if all of the following conditions are met:

- If used within a Certificate, such as the `signatureAlgorithm` field of a Certificate or the `signature` field of a TBSCertificate:
    - The new Certificate is a Root CA Certificate or Subordinate CA Certificate that is a Cross-Certificate; and,
    - There is an existing Certificate, issued by the same issuing CA Certificate, using the following encoding for the signature algorithm; and,
    - The existing Certificate has a `serialNumber` that is at least 64-bits long; and,
    - The only differences between the new Certificate and existing Certificate are one of the following:
        - A new `subjectPublicKey` within the `subjectPublicKeyInfo`, using the same algorithm and key size; and/or,
        - A new `serialNumber`, of the same encoded length as the existing Certificate; and/or
        - The new Certificate's `extKeyUsage` extension is present, has at least one key purpose specified, and none of the key purposes specified are the id-kp-serverAuth (OID: `1.3.6.1.5.5.7.3.1`) or the anyExtendedKeyUsage (OID: `2.5.29.37.0`) key purposes; and/or
        - The new Certificate's `basicConstraints` extension has a pathLenConstraint that is zero.
- If used within an OCSP response, such as the `signatureAlgorithm` of a BasicOCSPResponse:
    - The `producedAt` field value of the ResponseData MUST be earlier than 2022-06-01 00:00:00 UTC; and,
    - All unexpired, un-revoked Certificates that contain the Public Key of the CA Key Pair and that have the same Subject Name MUST also contain an `extKeyUsage` extension with the only key usage present being the id-kp-ocspSigning (OID: `1.3.6.1.5.5.7.3.9`) key usage.
- If used within a CRL, such as the `signatureAlgorithm` field of a CertificateList or the `signature` field of a TBSCertList:
    - The CRL is referenced by one or more Root CA or Subordinate CA Certificates; and,
    - The Root CA or Subordinate CA Certificate has issued one or more Certificates using the following encoding for the signature algorithm.

Note: The above requirements do not permit SSL.com to sign a Precertificate with this encoding.

- RSASSA-PKCS1-v1_5 with SHA-1:

  Encoding: `300d06092a864886f70d0101050500`

7.1.3.2.2 ECDSA

SSL.com SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is P-256, the signature MUST use ECDSA with SHA-256. When encoded, the `AlgorithmIdentifier` MUST be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040302`.

If the signing key is P-384, the signature MUST use ECDSA with SHA-384. When encoded, the `AlgorithmIdentifier` MUST be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040303`.

If the signing key is P-521, the signature MUST use ECDSA with SHA-512. When encoded, the `AlgorithmIdentifier` MUST be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040304`.

7.1.3.2.3 EdDSA

For S/MIME Certificates:

SSL.com SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is Curve25519, the signature algorithm SHALL be id-Ed25519 (OID: 1.3.101.112). When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300506032b6570`.

If the signing key is Curve448, the signature algorithm SHALL be id-Ed448 (OID: 1.3.101.113). When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300506032b6571`.

7.1.3.2.4 ML-DSA

For S/MIME Certificates:

SSL.com SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is ML-DSA-44, the signature algorithm SHALL be id-ml-dsa-44 (OID: 2.16.840.1.101.3.4.3.17). When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300b0609608648016503040311`.

If the signing key is ML-DSA-65, the signature algorithm SHALL be id-ml-dsa-65 (OID: 2.16.840.1.101.3.4.3.18). When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300b0609608648016503040312`.

If the signing key is ML-DSA-87, the signature algorithm SHALL be id-ml-dsa-87 (OID: 2.16.840.1.101.3.4.3.19). When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300b0609608648016503040313`.

7.1.4 Name forms

SSL.com Certificates support name chaining as specified in RFC 5280. All issued Certificates incorporate a unique identifying serial number.

7.1.4.1 Name Encoding

The content of the Certificate Issuer Distinguished Name field must match the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, Section 4.1.2.4.

For every valid Certification Path (as defined by RFC 5280, Section 6):

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

7.1.4.2 Subject Information - Subscriber Certificates

By issuing a Server Certificate, SSL.com represents that it followed the procedures set forth in this CP/CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. SSL.com shall not include a Domain Name or IP Address in a Subject attribute except as specified in §3.2.2.4 or §3.2.2.5. Subject attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

By issuing a Personal/Client/CodeSigning Certificate, SSL.com represents that it followed the procedures set forth in this CP/CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. SSL.com shall not include a commonName, emailAddress in a Subject attribute except as specified in §3.2.3. Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, SSL.com may use the `subject:organizationName` field to convey a natural person Subject's name or DBA.

See exceptions for Test Document Signing Certificates in §3.2.4.

7.1.4.2.1 Subject Alternative Name Extension

Certificate Field: extensions:subjectAltName

- Required/Optional:
  - **Required** for SSL (EV and non-EV), S/MIME and Mark Certificates
  - **Optional** for Code Signing and EV Code Signing Certificates

Contents for non-EV SSL Server Certificates: This extension must contain at least one entry. Each entry SHALL be one of the following types:

- `dNSName`: The entry SHALL contain either a Fully-Qualified Domain Name or Wildcard Domain Name that SSL.com has validated in accordance with §3.2.2.4. Wildcard Domain Names SHALL be validated for consistency with §3.2.2.6. The entry SHALL NOT contain an Internal Name. Underscore characters ("_") SHALL NOT be present in `dNSName` entries. Effective 2025-09-15, the entry MUST NOT contain an Address and Routing Parameter Area Name. Effective 2026-03-15, the entry MUST NOT contain a Domain Name that ends in an IP Address Reverse Zone Suffix.

  The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry SHALL be composed entirely of LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System SHALL NOT be included (e.g. "example.com" SHALL be encoded as "example.com" and SHALL NOT be encoded as "example.com.").

  The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name SHALL consist solely of Domain Labels that are P-Labels or Non-Reserved LDH Labels.

- `iPAddress`: The entry SHALL contain an IPv4 or IPv6 address that SSL.com has validated in accordance with §3.2.2.5. The entry SHALL NOT contain a Reserved IP Address.

Contents for EV SSL Server and Mark Certificates: This extension must contain at least one entry. Each entry SHALL be one of the following type:

- `dNSName`: The entry SHALL contain a Fully-Qualified Domain Name that SSL.com has validated in accordance with §3.2.2.4. The entry SHALL NOT contain an Internal Name. Underscore characters ("_") SHALL NOT be present in `dNSName` entries. This extension MUST NOT contain a Wildcard Domain Name unless the FQDN portion of the Wildcard Domain Name is an Onion Domain Name verified in accordance with Appendix B of the Baseline Requirements.

  The Fully-Qualified Domain Name contained in the entry SHALL be composed entirely of LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System SHALL NOT be included (e.g. "example.com" SHALL be encoded as "example.com" and SHALL NOT be encoded as "example.com.").

  Effective 2021-10-01, the Fully-Qualified Domain Name SHALL consist solely of Domain Labels that are P-Labels or Non-Reserved LDH Labels.

Contents for Code Signing and EV Code Signing Certificates: If this field is present, it shall not contain dNSName, iPAddress or other entries that point to a Domain Name or IP Address.

Contents for S/MIME Certificates: This extension must contain at least one entry. Each entry must be an rfc822Name containing an email address of the Subscriber. It must not contain a

Domain Name or IP Address. SSL.com must confirm that the Applicant controls the e-mail address as documented in §3.2.2.9.

7.1.4.2.2 Subject Distinguished Name Fields

a. Certificate Field: subject:commonName (OID 2.5.4.3)

- Required/Optional:
  - **Deprecated** (Discouraged, but not prohibited) for SSL (EV and non-EV) and Mark Certificates
  - **Required** for Code Signing or EV Code Signing Certificates
- **Contents for non-EV SSL Server Certificates:** If present, this field MUST contain exactly one entry that is one of the values contained in the Certificate's `subjectAltName` extension (see §7.1.4.2.1). The value of the field MUST be encoded as follows:
  - If the value is an IPv4 address, then the value MUST be encoded as an IPv4Address as specified in RFC 3986, Section 3.2.2.
  - If the value is an IPv6 address, then the value MUST be encoded in the text representation specified in RFC 5952, Section 4.
  - If the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value MUST be encoded as a character-for-character copy of the `dNSName` entry value from the `subjectAltName` extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels MUST NOT be converted to their Unicode representation.
- **Contents for EV SSL Server Certificates:** If present, this field MUST contain exactly one entry that is one of the values contained in the Certificate's `subjectAltName` extension (see §7.1.4.2.1). The value of the field MUST be encoded as follows:
  - If the value is a Fully-Qualified Domain Name, then the value MUST be encoded as a character-for-character copy of the `dNSName` entry value from the `subjectAltName` extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name must be encoded as LDH Labels, and P-Labels MUST NOT be converted to their Unicode representation.
- **Contents for Code Signing Certificates:** This field must contain the Subject's legal name as verified under §3.2.2.2.
- **Contents for EV Code Signing Certificates:** This field must contain the Subject's legal name as verified under Section 3.2.2.2 of the EV Guidelines. SSL.com must ensure that this name does not constitute a valid Domain Name or IP Address.
- **Contents for S/MIME Certificates:** If present, this field must include one of the following values verified in accordance with §3.2:
  - **Mailbox-validated**: Mailbox Address
  - **Organization-validated**: `subject:organizationName` or Mailbox Address
  - **Sponsor-validated**: Personal Name or Mailbox Address
  - **Individual-validated**: Personal Name or Mailbox Address

- **Contents for Mark Certificates:** If present this field must include either the Subject Organization Name defined in §7.1.4.2.2 (b) or the Word Mark field defined in §7.1.4.2.2 (s).

b. Certificate Field: subject:organizationName (OID 2.5.4.10)

- Required/Optional:
  - **Optional** for non-OV SSL, non-EV SSL or S/MIME Certificates
  - **Required** for OV SSL, EV SSL, Code Signing or EV Code Signing Certificates
- **Contents for non-EV SSL Certificates:** If present, the `subject:organizationName` field must contain either the Subject's name and/or DBA/tradename as verified under §3.2.2.2. SSL.com may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that SSL.com documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", SSL.com may use "Company Name Inc." or "Company Name". Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, SSL.com may use the `subject:organizationName` field to convey a natural person Subject's name and/or DBA/tradename. If both are included, the DBA/tradename SHALL appear first, followed by the Subject's name in parentheses.
- **Contents for Code Signing or S/MIME Certificates:** If present, the `subject:organizationName` field must contain either the Subject's name or DBA as verified under §3.2.2.2. SSL.com may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that SSL.com documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", SSL.com may use "Company Name Inc." or "Company Name". Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, SSL.com may use the `subject:organizationName` field to convey a natural person Subject's name or DBA.
- **Contents for EV Server or EV Code Signing Certificates:** This field must contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by SSL.com as provided herein. SSL.com may abbreviate the organization prefixes or suffixes in the organization name, e.g., if the official record shows "Company Name Incorporated" SSL.com may include "Company Name, Inc". When abbreviating a Subject's full legal name as allowed by this subsection, SSL.com must use abbreviations that are not misleading in the Jurisdiction of Incorporation or Registration. In addition, an assumed name or DBA name used by the Subject may be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis.
- If the combination of names or the organization name by itself exceeds 64 characters, SSL.com may abbreviate parts of the organization name, and/or omit non-material

words in the organization name in such a way that the text in this field does not exceed the 64-character limit. SSL.com shall check this field in accordance with §4.2.1 and a Relying Party will not be misled into thinking that they are dealing with a different organization.

c. Certificate Field: subject:givenName (2.5.4.42) and subject:surname (2.5.4.4)

- **Contents:** If present, the `subject:givenName` field and `subject:surname` field MUST contain a natural person Subject's name as verified under §3.2.3. A TLS Certificate containing a `subject:givenName` field or `subject:surname` field MUST contain the (`2.23.140.1.2.3`) Certificate Policy OID.

d. Certificate Field: Number and street: subject:streetAddress (OID: 2.5.4.9)

- Required/Optional:
  - **Required** for Mark Certificates
  - **Optional** if the `subject:organizationName` field, `subject:givenName` field, or `subject:surname` field are present.
  - **Prohibited** if the `subject:organizationName` field, subject:givenName, and `subject:surname` field are absent.
- **Contents for non-EV SSL, Code Signing or S/MIME Certificates:** If present, the `subject:streetAddress` field must contain the Subject's street address information as verified under §3.2.2.1.
- **Contents for EV Server, EV Code Signing or Mark Certificates:** If present, the `subject:streetAddress` field must contain the physical location of the Subject's Place of Business as verified under §3.2.2.1.

e. Certificate Field: subject:localityName (OID: 2.5.4.7)

- Required/Optional:
  - **Required** if the `subject:organizationName` field, `subject:givenName` field, or `subject:surname` field are present and the `subject:stateOrProvinceName` field is absent.
  - **Optional** if the `subject:stateOrProvinceName` field and the `subject:organizationName` field, `subject:givenName` field, or `subject:surname` field are present.
  - **Prohibited** if the `subject:organizationName` field, subject:givenName, and `subject:surname` field are absent.
- **Contents:** If present, the `subject:localityName` field must contain the Subject's locality information as verified under §3.2.2.1. If the `subject:countryName` field specifies the ISO 3166-1 user-assigned code of XX in accordance with §7.1.4.2.2(h), the localityName field may contain the Subject's locality and/or state or province information as verified under §3.2.2.1.

f. Certificate Field: subject:stateOrProvinceName (OID: 2.5.4.8)

- Required/Optional:
  - **Required** if the `subject:organizationName` field, `subject:givenName` field, or `subject:surname` field are present and `subject:localityName` field is absent.

    - **Optional** if the `subject:localityName` field and the `subject:organizationName` field, the `subject:givenName` field, or the `subject:surname` field are present.
    - **Prohibited** if the `subject:organizationName` field, the `subject:givenName` field, or `subject:surname` field are absent.
- **Contents:** If present, the `subject:stateOrProvinceName` field must contain the Subject's state or province information as verified under §3.2.2.1. If the `subject:countryName` field specifies the ISO 3166-1 user-assigned code of XX in accordance with §7.1.4.2.2(h), the `subject:stateOrProvinceName` field may contain the full name of the Subject's country information as verified under §3.2.2.1.

g. Certificate Field: subject:postalCode (OID: 2.5.4.17)

- Required/Optional:
    - **Optional** if the subject:organizationName, `subject:givenName` field, or `subject:surname` fields are present.
    - **Prohibited** if the `subject:organizationName` field, `subject:givenName` field, or `subject:surname` field are absent.
- **Contents:** If present, the `subject:postalCode` field must contain the Subject's zip or postal information as verified under §3.2.2.1.

h. Certificate Field: subject:countryName (OID: 2.5.4.6)

- Required/Optional:
    - **Required** if the `subject:organizationName` field, subject:givenName, or `subject:surname` field are present. It is always required for EV Server Certificates.
    - **Optional** if the `subject:organizationName` field, `subject:givenName` field, and `subject:surname` field are absent.
- **Contents for non-EV SSL, Code Signing or S/MIME Certificates:** If the `subject:organizationName` field is present, the `subject:countryName` must contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under §3.2.2.1. If the `subject:organizationName` field is absent, the `subject:countryName` field may contain the two-letter ISO 3166-1 country code associated with the Subject as verified in accordance with §3.2.2.3. If a Country is not represented by an official ISO 3166-1 country code, SSL.com may specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.
- **Contents for EV server, EV Code Signing or Mark Certificates:** This field must contain the two-letter ISO 3166-1 country code associated with the physical location of the Subject's Place of Business as verified under the EV Guidelines. If a Country is not represented by an official ISO 3166-1 country code, SSL.com may specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

i. Certificate Field: subject:organizationalUnitName (OID: 2.5.4.11)

- Required/Optional:

- **Optional** for non-TLS certificates
- **Prohibited** for Server TLS Certificates.

SSL.com shall implement a process that prevents an OU attribute from including a name, DBA, trade name, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless SSL.com has verified this information in accordance with §3.2 and the Certificate also contains subject:organizationName, subject:localityName, and `subject:countryName` attributes, also verified in accordance with §3.2.2.1.

For Mark Certificates the Organizational Unit Name field identifies an organizational unit with which the certificate is affiliated. The designated organizational unit is understood to be part of an organization designated by a `subject:organizationName` field. The value for Organizational Unit Name is a string chosen by the organization of which it is part (e.g., OU = Technology Division). See ISO/IEC 9594-6:2014 (E) Rec. ITU-T X.520 (10/2012).

j. Certificate Field: subject:organizationIdentifier (OID: 2.5.4.97)

- Required/Optional:
  - **Required** for OV and SV S/MIME certificates.
  - **Optional** for other types of certificates.
- **Contents:** If present, the `subject:organizationIdentifier` SHALL be encoded as a PrintableString or UTF8String, and it SHALL contain a Registration Reference to the Legal Entity assigned in accordance to the identified Registration Scheme. The Registration Reference SHOULD be unique where the Registration Scheme and jurisdiction provide unique identifiers.
  - **S/MIME Certificates:** For S/MIME certificates, the organizationIdentifier SHALL be validated in accordance with Section 3.2.3 of the S/MIME Baseline Requirements and it SHALL be assigned in accordance to one of the Registration Scheme of Appendix A of S/MIME Baseline Requirements.
  - **Mark Certificates:** For MCs, the organizationIdentifier SHALL be validated in accordance with Section 7.1.4.2.2 (q) of the MC Requirements and it SHALL be assigned in accordance to one of the Registration Scheme of Appendix J of the MC Requirements.

k. Other Subject Attributes

- Other attributes MAY be present within the subject field. If present, other attributes MUST contain information that has been verified by SSL.com.
- For EV SSL and Code Signing Certificates, SSL.com SHALL NOT include any Subject Distinguished Name attributes except as specified in §9.2

Special Subject Attributes for EV and Mark Certificates

The following Subject Attributes are applicable for EV SSL, EV Code Signing and Mark Certificates Certificates according to the EV and MC Guidelines.

l. Certificate field: subject:businessCategory (OID: 2.5.4.15)

- Required/Optional: **Required**
- **Contents:** This field MUST contain one of the following strings: “Private Organization”, “Government Entity”, “Business Entity”, or “Non-Commercial Entity” depending upon whether the Subject qualifies under the terms of Section 4.1.1.1, 4.1.1.2, 4.1.1.3 or 4.1.1.4 of the EV Guidelines, respectively.

m. Subject Jurisdiction of Incorporation or Registration field

- **Certificate fields:**
    - Locality (if required): *subject:jurisdictionLocalityName* (OID: `1.3.6.1.4.1.311.60.2.1.1`)
    - State or province (if required): *subject:jurisdictionStateOrProvinceName* (OID: `1.3.6.1.4.1.311.60.2.1.2`)
    - Country: *subject:jurisdictionCountryName* (OID: `1.3.6.1.4.1.311.60.2.1.3`)
- Required/Optional: **Required**
- **Contents:** These fields MUST NOT contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. For example, the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level MUST include the country information but MUST NOT include the state or province or locality information. Similarly, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information, but MUST NOT include locality information. And, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information. Country information MUST be specified using the applicable ISO country code. State or province or locality information (where applicable) for the Subject’s Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction.
- SSL.com SHALL disclose, at time of issuance, the values within these fields within the latest publicly-available disclosure, as described in the EV Guidelines Section 3.2.2.1.3, as acceptable values for the applicable Incorporating Agency or Registration Agency.

n. Certificate field: subject:serialNumber (OID: 2.5.4.5)

- Required/Optional: **Required**
- **Contents:** For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.

    - For Government Entities that do not have a Registration Number or readily verifiable date of creation, SSL.com SHALL enter appropriate language to indicate that the Subject is a Government Entity.
    - For Business Entities, the Registration Number that was received by the Business Entity upon government registration SHALL be entered in this field. For those Business Entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration SHALL be entered into this field in any one of the common date formats.
- If SSL.com has disclosed a set of acceptable format or formats for Registration Numbers for the applicable Registration Agency or Incorporating Agency, as described in the EV Guidelines Section 3.2.2.1.3, SSL.com SHALL ensure, prior to issuance, that the Registration Number is valid according to at least one currently disclosed format for that applicable Registration Agency or Incorporating agency.

o. Certificate field: subject:trademarkOfficeName (OID: 1.3.6.1.4.1.53087.1.2)

- Required/Optional:
    - **Required** if the `subject:markType` field contains one of the following values: "Registered Mark" or "Modified Registered Mark" and the applicable country/region has more than one national/regional intellectual property agency where trademarks can be registered;
    - **Optional** if the `subject:markType` otherwise contains one of the following values: "Registered Mark" or "Modified Registered Mark";
    - **Prohibited** if the `subject:markType` does not contain one of the following values: "Registered Mark" or "Modified Registered Mark".
- **Contents:** This string value identifies the Trademark Office by inserting the Trademark Office name listed in the "Office" column in the WIPO directory of country and regional intellectual property agencies at https://www.wipo.int/directory/en/urls.jsp for the Trademark Office that registered the Registered Mark included in the Mark Certificate or is processing the application of the Mark included in the Mark Certificate.

p. Certificate field: subject:trademarkCountryOrRegionName (OID: 1.3.6.1.4.1.53087.1.3)

- Required/Optional:
    - **Required** if the `subject:markType` field contains one of the following values: "Registered Mark" or "Modified Registered Mark";
    - **Prohibited** otherwise.
- **Contents:** If the `subject:markType` field contains "Registered Mark" or "Modified Registered Mark", then this field MUST contain the country or region of the Trademark Office that registered the Registered Mark as an WIPO ST.3 two letter country and intergovernmental/regional agency code (see list at https://www.wipo.int/export/sites/www/standards/en/pdf/03-03-01.pdf).

q. Certificate field: subject:trademarkIdentifier (OID: 1.3.6.1.4.1.53087.1.4)

- Required/Optional:

    - **Required** if the `subject:markType` field contains one of the following values: "Registered Mark" or "Modified Registered Mark";
    - **Prohibited** otherwise.
- **Contents:** This string value contains the identifier assigned by the Trademark Office to identify the Registered Mark or Registered Mark application.

r. Certificate field: subject:legalEntityIdentifier (OID: 1.3.6.1.4.1.53087.1.5)

- Required/Optional: **Optional**
- **Contents:** Contains a 20-character alphanumeric LEI string from a valid registration. The validation process for Mark Certificates is as follows:
    1. This information SHALL be validated by matching the organization name and registration number found in the Global LEI Index against the Subject Organization Name Field (see §7.1.4.2.2 (b)) and Subject Serial Number Field (see §7.1.4.2.2 (n)) within the context of the subject's jurisdiction as specified in §7.1.4.2.2 (m)). The address information from Mark validation SHALL be compared to the Headquarters Address information in the LEI record in order to detect potential matching errors or errors in the registration information. If the addresses do not match, SSL.com will attempt to validate the address found in the LEI record as a confirmed office location for the Subscriber, if possible.
    2. SSL.com SHALL verify that the ValidationSources field of the associated LEI record contains the designation FULLY_CORROBORATED before including an LEI in a MC.

s. Certificate field: subject:wordMark (OID: 1.3.6.1.4.1.53087.1.6)

- Required/Optional: **Optional**
- **Contents:** Contains a Word Mark or the word(s) included in a Combined Mark.

t. Certificate field: subject:markType (OID: 1.3.6.1.4.1.53087.1.13)

- Required/Optional: **Required**
- **Contents:** This field MUST contain one of the values corresponding to Section 3.2.16 or Section 3.2.17 of the MC Requirements that SSL.com employed to validate the Mark included in the Certificate: "Registered Mark", "Government Mark", "Prior Use Mark", "Modified Registered Mark".

u. Subject Jurisdiction of Government Entity that established the Government Mark

- **Certificate fields:**
    - Locality (if required): subject:statuteLocalityName (OID: 1.3.6.1.4.1.53087.3.4)
    - State or province (if required): subject:statuteStateOrProvinceName (OID: 1.3.6.1.4.1.53087.3.3)
    - Country: subject:statuteCountryName (OID: 1.3.6.1.4.1.53087.3.2)
- Required/Optional: **Required** if the subject:markType field contains "Government Mark"; **Prohibited** otherwise
- **Contents:** Certificates MUST NOT contain these fields unless they are relevant to the level of the Government Entity or Non-Commercial Entity (International Organization)

that established the Government Mark through statute, regulation, treaty, or government action.

For example, the jurisdiction for a Government Entity or Non-Commercial Entity (International Organization) that operates at the country level MUST include the statuteCountry field but MUST NOT include the statuteStateOrProvince and statuteLocality fields.

Similarly, the jurisdiction for the applicable Government Entity or Non-Commercial Entity (International Organization) at the state or province level MUST include both statuteCountry and statuteStateOrProvince fields but MUST NOT include the statuteLocality field. And, the jurisdiction for the applicable Government Entity or Non-Commercial Entity (International Organization) at the locality level MUST include the statuteCountry and statuteStateOrProvince fields, where the state or province regulates the registration of the entities at the locality level, as well as the statuteLocality field.

statuteCountry field values MUST be specified using the applicable ISO country code.

statuteStateOrProvince and statuteLocality field values (where applicable) MUST be specified using the full name of the applicable jurisdiction.

v. Certificate field: subject:statuteCitation (OID: 1.3.6.1.4.1.53087.3.5)

- Required/Optional: **Required** if the subject:markType field contains "Government Mark"; **Prohibited** otherwise
- **Contents:** If the Certificates contains a Mark verified in accordance with Section §3.2.2.12, then this field MUST include the official statute, regulation, treaty, or government action by which the Government Mark was granted or claimed, as confirmed by the CA. The field may contain common abbreviations, and SHOULD conform, if possible, to applicable legal guidelines in the jurisdiction for how such official statutes, regulations, or government actions are normally cited (e.g., "The Bluebook: A Uniform System of Citation" or other similar standard system of citation.)

In addition, SSL.com MAY include brief explanatory text to assist Relying Parties in locating the official statute, regulation, treaty, or government action by which the Government Mark was granted or claimed.

w. Certificate field: subject:statuteURL (OID: 1.3.6.1.4.1.53087.3.6)

- Required/Optional: **Optional** if the subject:markType field contains "Government Mark"; **Prohibited** otherwise
- **Contents:** If present, this field MUST contain a HTTP/HTTPS URL where the official statute, regulation, treaty, or government action by which the Government Mark was granted or claimed can be found.

x. Certificate field: subject:priorUseMarkSourceURL (OID: 1.3.6.1.4.1.53087.5.1)

If the subject:markType field contains "Prior Use Mark": - Required/Optional: **Optional** if the Common Mark Certificate is issued before April 15, 2025; **Required** if the Common Mark Certificate is issued on or after April 15, 2025 - **Contents:** This field MUST contain the URL

where the Mark Representation included in the Mark Certificate was located by the CA during the verification process.

7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates

By issuing a Subordinate CA Certificate, SSL.com represents that it followed the procedure set forth in this CP/CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.1 Subject Distinguished Name Fields

a. Certificate Field: subject:commonName (OID 2.5.4.3)

- Required/Optional: **Required**
- **Contents:** This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.

b. Certificate Field: subject:organizationName (OID 2.5.4.10)

- Required/Optional: **Required**
- **Contents:** This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under §3.2.2.2. SSL.com may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that SSL.com documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", SSL.com MAY use "Company Name Inc." or "Company Name".

c. Certificate Field: subject:countryName (OID: 2.5.4.6)

- Required/Optional: **Required**
- **Contents:** This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.

7.1.5 Name Constraints

SSL.com reserves the right to issue Certificates with name constraints and/or marked as critical when deemed necessary.

If SSL.com decides to apply Name Constraints and if the Subordinate CA Certificate includes the `id-kp-serverAuth` RFC 5280 extended key usage, then the Subordinate CA Certificate must include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

a. For each dNSName in permittedSubtrees, SSL.com must confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of §3.2.2.4.
b. For each iPAddress range in permittedSubtrees, SSL.com must confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.

c. For each DirectoryName in permittedSubtrees SSL.com must confirm the Applicant's and/or Subsidiary's Organizational name and location such that end entity Certificates issued from the subordinate CA Certificate will be in compliance with §7.1.2.4 and §7.1.2.5.

If the Subordinate CA Certificate is not allowed to issue Certificates with an iPAddress, then the Subordinate CA Certificate must specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate must include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate must also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate must include at least one iPAddress in permittedSubtrees.

A decoded example for issuance to the domain and sub domains of example.com by organization: "Example LLC, Boston, Massachusetts, US" would be:

X509v3 Name Constraints:
> Permitted:
> > DNS:example.com
> > DirName: C=US, ST=MA, L=Boston, O=Example LLC
> Excluded:
> > IP:0.0.0.0/0.0.0.0
> > IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

If the Subordinate CA is not allowed to issue Certificates with dNSNames, then the Subordinate CA Certificate must include a zero-length dNSName in excludedSubtrees. Otherwise, the Subordinate CA Certificate must include at least one dNSName in permittedSubtrees.

7.1.6 Certificate Policy object identifier

The OID (Object Identifier) of this CP/CPS is documented in §1.2.1.

A special OID arc has been allocated by SSL.com based on a certain certificate type:

iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) SSL.com (38064) certificationServicesProvision (1) certificateTypes (3)

SSL.com issues Certificates containing the following OIDs / OID arcs:

Digitally Signed Object	Policy Object Identifier (OID)
TLS Server Authentication Certificates	**1.3.6.1.4.1.38064.1.3.1**
Domain Validation (DV) Policy, and IP address validation compatible with CA/B Forum Policy OID `2.23.140.1.2.1`	**1.3.6.1.4.1.38064.1.3.1.1**

Digitally Signed Object	Policy Object Identifier (OID)
Organization Validation (OV) Policy compatible with CA/B Forum Policy OID `2.23.140.1.2.2`	**1.3.6.1.4.1.38064.1.3.1.2**
Individual Validation (IV) Policy compatible with CA/B Forum Policy OID `2.23.140.1.2.3`	**1.3.6.1.4.1.38064.1.3.1.3**
Extended Validation (EV) Policy compatible with CA/B Forum Policy OID `2.23.140.1.1.`	**1.3.6.1.4.1.38064.1.3.1.4**
NAESB Server Cert Basic Assurance compatible with CA/B Forum OV Policy OID `2.23.140.1.2.2` and NAESB Policy OID `2.16.840.1.114505.1.12.2.2.`	**1.3.6.1.4.1.38064.1.3.1.5**
NAESB Server Cert Medium Assurance compatible with CA/B Forum EV Policy OID `2.23.140.1.1` and NAESB Policy OID `2.16.840.1.114505.1.12.3.2.`	**1.3.6.1.4.1.38064.1.3.1.6**
S/MIME Signing/Encryption Certificates	**1.3.6.1.4.1.38064.1.3.2**
Email Address Validation, i.e. email address only, compatible with CA/B Forum Policy OID `2.23.140.1.5.1` (*mailbox-validated*)	**1.3.6.1.4.1.38064.1.3.2.1**
Email Address and Organization Validation, i.e. email address plus the Organization information, compatible with CA/B Forum Policy OID `2.23.140.1.5.2` (*organization-validated*), or the Individual information plus information of the affiliated Organization, compatible with CA/B Forum Policy OID `2.23.140.1.5.3` (*sponsor-validated*)	**1.3.6.1.4.1.38064.1.3.2.2**
Email Address and Individual Validation, i.e. email address plus the Individual information without any affiliation, compatible with CA/B Forum Policy OID `2.23.140.1.5.4` (*individual-validated*)	**1.3.6.1.4.1.38064.1.3.2.3**
Code Signing Certificates	**1.3.6.1.4.1.38064.1.3.3**
Minimum Requirements for Code Signing Policy, compatible with CA/B Forum Policy OID `2.23.140.1.4.1`	**1.3.6.1.4.1.38064.1.3.3.1**
Extended Validation (EV) Code Signing Policy, compatible with CA/B Forum Policy OID `2.23.140.1.3`	**1.3.6.1.4.1.38064.1.3.3.2**
Document Signing Certificates	**1.3.6.1.4.1.38064.1.3.4**
Organization Validation (e.g. the full name of individual associated with a particular Organization, or just the Organization information)	**1.3.6.1.4.1.38064.1.3.4.1**
Individual Validation (e.g. the full name of individual only)	**1.3.6.1.4.1.38064.1.3.4.2**
Email Validation (i.e. the email address only)	**1.3.6.1.4.1.38064.1.3.4.3**

Digitally Signed Object	Policy Object Identifier (OID)
Test Certificate, compatible with Adobe AATL Policy OID 1.2.840.113583.1.2.2	**1.3.6.1.4.1.38064.1.3.4.4**
Client Authentication Certificates	**1.3.6.1.4.1.38064.1.3.5**
Organization Validation (e.g. the full name of individual associated with a particular Organization, or just the Organization information)	**1.3.6.1.4.1.38064.1.3.5.1**
Individual Validation (e.g. the full name of individual only)	**1.3.6.1.4.1.38064.1.3.5.2**
Rudimentary Assurance Validation for NAESB, compatible with NAESB Rudimentary Assurance Policy OID 2.16.840.1.114505.1.12.1.2	**1.3.6.1.4.1.38064.1.3.5.3**
Basic Assurance Validation for NAESB, compatible with NAESB Basic Assurance Policy OID 2.16.840.1.114505.1.12.2.2	**1.3.6.1.4.1.38064.1.3.5.4**
Medium Assurance Validation for NAESB, compatible with NAESB Medium Assurance Policy OID 2.16.840.1.114505.1.12.3.2	**1.3.6.1.4.1.38064.1.3.5.5**
High Assurance Validation for NAESB, compatible with NAESB High Assurance Policy OID 2.16.840.1.114505.1.12.4.2	**1.3.6.1.4.1.38064.1.3.5.6**
Email Address validation only	**1.3.6.1.4.1.38064.1.3.5.7**
Time-Stamping	**1.3.6.1.4.1.38064.1.3.6**
Basic Time-Stamping, compatible with CA/B Forum Policy OID 2.23.140.1.4.2	**1.3.6.1.4.1.38064.1.3.6.1**
EV Time-Stamping, compatible with CA/B Forum Policy OID 2.23.140.1.4.2	**1.3.6.1.4.1.38064.1.3.6.2**
Time-stamping Certificate for Document Signing Trust	**1.3.6.1.4.1.38064.1.3.6.3**
OCSP Responder Certificate	**1.3.6.1.4.1.38064.1.3.7**
Mark Certificates, compatible with BIMI Group Mark Certificate General Policy Identifier(1.3.6.1.4.1.53087.1.1)	**1.3.6.1.4.1.38064.1.3.8**

These SSL.com custom Policy OIDs are used when Certificates are signed pursuant to this CP/CPS are indicated in the certificate's respective certificatePolicies extension. When a Certificate is issued containing a certain policy identifier which is indicated as compatible with the "CA/B Forum Policy OID X" or "NAESB Policy OID X", it asserts that the Certificate was issued and is managed in accordance with those applicable requirements AND the provisions of this CP/CPS.

TLS Subscriber Certificates MUST contain, within the Certificate's certificatePolicies extension, one or more policy identifier(s) that are specified beneath the CA/Browser Forum's reserved policy OID arc of {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1)} (2.23.140.1).

Subordinate CAs that are Affiliated with SSL.com can use the reserved `AnyPolicy` OID **2.5.29.32.0**.

If the Certificate asserts the policy identifier `2.23.140.1.2.1` (DV TLS Server Certificate), then it MUST NOT include organizationName, givenName, surname, streetAddress, localityName, stateOrProvinceName, or postalCode in the Subject field.

If the Certificate asserts the policy identifier `2.23.140.1.2.2` (OV TLS Server Certificate), then it MUST also include organizationName, localityName and/or stateOrProvinceName, and countryName in the Subject field.

If the Certificate asserts the policy identifier `2.23.140.1.2.3` (IV TLS Server Certificate), then it MUST also include givenName, surname, localityName and/or stateOrProvinceName, and countryName in the Subject field.

If the Certificate asserts the policy identifier `2.23.140.1.1` (EV TLS Server Certificate), then it MUST also include Subject Identity Information as required and verified according to the EV Guidelines.

If the Certificate asserts the policy identifier `1.3.6.1.4.1.38064.1.3.2.1` (Email address only S/MIME Certificate), then it MUST NOT include organizationName, givenName, surname, streetAddress, localityName, stateOrProvinceName or postalCode in the Subject field.

If the Certificate asserts the policy identifier `1.3.6.1.4.1.38064.1.3.2.2` and `2.23.140.1.5.2` (Organization Validated S/MIME Certificate), then it MUST also include organizationName, localityName and/or stateOrProvinceName, and countryName in the Subject field.

If the Certificate asserts the policy identifier `1.3.6.1.4.1.38064.1.3.2.2` and `2.23.140.1.5.3` (Sponsor Validated S/MIME Certificate), then it MUST also include givenName, surname, organizationName, localityName and/or stateOrProvinceName, and countryName in the Subject field.

If the Certificate asserts the policy identifier `1.3.6.1.4.1.38064.1.3.2.3` (Individual Validated S/MIME Certificate), then it MUST also include givenName, surname and countryName in the Subject field.

If the Certificate asserts the policy identifier `1.3.6.1.4.1.38064.1.3.4.1` (Organization Validated Document Signing Certificate), then it MUST also include organizationName, localityName and/or stateOrProvinceName, and countryName in the Subject field.

If the Certificate asserts the policy identifier `1.3.6.1.4.1.38064.1.3.4.2` (Individual Validated Document Signing Certificate), then it MUST also include givenName, surname and countryName in the Subject field.

If the Certificate asserts the policy identifier `1.2.840.113583.1.2.2` (Test Document Signing Certificate), then it MUST also include the words “Test Certificate - Not to be relied upon” in the Subject field.

7.1.7 Usage of Policy Constraints extension

No stipulation

7.1.8 Policy qualifiers syntax and semantics

SSL.com's policy qualifier field includes information relying parties may consult in order to determine any limitations a certificate may have.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation

7.2 CRL Profile

7.2.1 Version Numbers

SSL.com's PKI issues version 2 CRLs which comply with RFC 5280 and contain the following:

- Issuer Signature Algorithm: The algorithm used to sign the CRL.
- Issuer Distinguished Name: The Distinguished Name of the Certification Authority that has signed and issued the CRL, matched byte-for-byte.
- thisUpdate: Issue date of the CRL in UTCTime or GeneralizedTime.
- nextUpdate: Date by which the next CRL will be issued in UTCTime or GeneralizedTime.
- Revocation list (Identified by certificate serial number): List of all revoked Certificates including their serial number and the date and time of the revocation in UTCTime or GeneralizedTime.
- Serial Number
- Issuer's Signature

7.2.2 CRL and CRL Entry Extensions

CRL and CRL Entry Extensions follow the requirements of section 5 of RFC 5280.

If a CRL has a thisUpdate field value of 2022-07-01 00:00:00 UTC or later and the CA includes the Invalidity Date CRL entry extension in a CRL entry for a Code Signing Certificate, then the time encoded in the Invalidity Date CRL extension SHALL be equal to the time encoded in the revocationDate field of the CRL entry.

7.2.2.1 CRL Number

Sequentially increasing unique number for each CRL.

7.2.2.2 Authority Key Identifier

The Authority Key Identifier of an issuing CA used for chaining and validation.

7.2.2.3 Revocation reasonCode (OID 2.5.29.21)

If present, this extension MUST NOT be marked critical.

If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates technically capable of issuing TLS Certificates, this CRL entry extension MUST be present.

If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension SHOULD be present, but MAY be omitted, subject to the following requirements.

The CRLReason indicated MUST NOT be unspecified (0). If the reason for revocation is unspecified, CAs MUST omit reasonCode entry extension, if allowed by the previous requirements.

If a CRL entry is for a TLS or a Code Signing Certificate, the CRLReason MUST NOT be certificateHold (6).

If a reasonCode CRL entry extension is present, the CRLReason MUST indicate the most appropriate reason for revocation of the certificate (see §4.9.1.1 and §4.9.1.2).

CRLReason MUST be included in the reasonCode extension of the CRL entry corresponding to a Subscriber TLS Server Certificate that is revoked after July 15, 2023, unless the CRLReason is "unspecified (0)". Revocation reason code entries for Subscriber TLS Server Certificates revoked prior to July 15, 2023, do NOT need to be added or changed.

Only the following CRLReasons MAY be present in the CRL reasonCode extension for Subscriber TLS or Code Signing Certificates:

- **keyCompromise (RFC 5280 CRLReason #1):** Indicates that it is known or suspected that the Subscriber's Private Key has been compromised;
- **affiliationChanged (RFC 5280 CRLReason #3):** Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised;
- **superseded (RFC 5280 CRLReason #4):** Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with these Baseline Requirements or the CA's CP or CPS;
- **cessationOfOperation (RFC 5280 CRLReason #5):** Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate; or
- **privilegeWithdrawn (RFC 5280 CRLReason #9):** Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or

has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

The Subscriber Agreement, or an online resource referenced therein, MUST inform Subscribers of TLS or Code Signing Certificates about the revocation reason options listed above and provide explanation about when to choose each option. Tools that SSL.com provides to the Subscribers of TLS or Code Signing Certificates MUST allow for these options to be easily specified when the Subscriber requests revocation of their TLS or Code Signing Certificate, with the default value being that no revocation reason is provided (i.e. the default corresponds to the CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL).

The privilegeWithdrawn reasonCode SHOULD NOT be made available to the Subscriber as a revocation reason option, because the use of this reasonCode is determined by SSL.com and not the Subscriber.

When SSL.com obtains verifiable evidence of Key Compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, SSL.com SHOULD update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension. Additionally, SSL.com SHOULD update the revocation date in a CRL entry when it is determined that the private key of the certificate was compromised prior to the revocation date that is indicated in the CRL entry for that certificate.

Note: Backdating the revocationDate field is an exception to best practice described in RFC 5280 (section 5.3.2); however, these requirements specify the use of the revocationDate field to support TLS and Code Signing implementations that process the revocationDate field as the date when the Certificate is first considered to be compromised.

7.2.2.4 `issuingDistributionPoint` (OID 2.5.29.28)

Effective 2023-01-15, if a CRL does not contain entries for all revoked unexpired certificates issued by the CRL issuer, then it MUST contain a critical Issuing Distribution Point extension and MUST populate the `distributionPoint` field of that extension.

7.3 OCSP Profile

SSL.com's PKI system operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 5019 and highlights this via an OCSP responder URL. OCSP version 1 defined by RFC 6960 is also supported.

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the `revocationReason` field within the `RevokedInfo` of the `CertStatus` MUST be present.

The `CRLReason` indicated MUST contain a value permitted for CRLs, as specified in §7.2.2.3.

7.3.1 Version Numbers

SSL.com's OCSP responders conform to version 1 of RFC 6960.

7.3.2 OCSP Extensions

The `singleExtensions` of an OCSP response MUST NOT contain the `reasonCode` (OID `2.5.29.21`) CRL entry extension.

The `singleExtensions` of an OCSP response MAY contain the `ArchiveCutOff` (OID `1.3.6.1.5.5.7.48.1.6`) as described in section 4.4.4 of RFC 6960 with values according to §4.10.1 of this CP/CPS.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

SSL.com's operations and practices meet or exceed generally accepted industry standards (including the requirements described in §8.4). This is ensured by the implementation of regularly scheduled external assessments and audits, as well as ongoing internal assessments and audits.

8.1 Frequency or circumstances of assessment

SSL.com is audited on an annual basis in order to ensure compliance with the standards identified in this section. Audits are performed by a Qualified Auditor and cover all SSL.com activities.

8.2 Identity/qualifications of assessor

Any external audit shall be performed by a Qualified Auditor who can demonstrate the following:

- Independence from the subject of the audit
- The ability to conduct an audit that addresses the criteria specified in an eligible audit scheme as stipulated in §8.4
- The employment of individuals proficient in the examination of Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function
- Status as certified, accredited, licensed, or otherwise meeting the qualification requirements of auditors under the audit scheme
- Adherence to applicable laws, government regulation, and professional code of ethics
- Maintains Professional Liability/Errors & Omissions insurance with a minimum of one million ($1,000,000) US dollars in coverage.

8.3 Assessor's relationship to assessed entity

Any external auditor shall be independent from any relationships that might constitute a conflict of interest, or that could in any way impair the external auditor's objective assessment.

8.4 Topics covered by assessment

8.4.1 CA assessment

SSL.com shall undergo a conformity assessment audit for compliance with the following requirements:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
- CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
- CA/Browser Forum Network and Certificate System Security Requirements
- BIMI Group Minimum Security Requirements for Issuance of Mark Certificates

in accordance with the latest applicable versions of the following schemes:

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline
- WebTrust Principles and Criteria for Certification Authorities - Network Security
- WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities - Code Signing Baseline Requirements
- WebTrust Principles and Criteria for Certification Authorities - S/MIME Certificates
- WebTrust Principles and Criteria for Certification Authorities - Mark Certificates

Relevant aspects of SSL.com's operations undergo regularly scheduled external audits which adhere to all of the industry standards listed in chapter 8. These audits are conducted by a Qualified Auditor, as specified in §8.2.

Internal audits and assessments, as described in §8.7, shall address all aspects of SSL.com's operations as required to ensure integrity and security.

Audits MUST be conducted for all obligations under this CP/CPS, including the operations of Timestamp Authorities and Signing Services.

For Delegated Third Parties which are not Enterprise RAs, SSL.com SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in this §8.4, which provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or SSL.com's CP/CPS.

If the opinion is that the Delegated Third Party does NOT comply with the above requirements, then SSL.com SHALL NOT allow the Delegated Third Party to continue performing delegated functions.

The audit period for any Delegated Third Party SHALL NOT exceed one year (ideally aligned with SSL.com's audit).

For Enterprise RAs participating in the validation of S/MIME Certificates:

- An annual audit that meets the criteria specified in §8.4 SHALL apply, or
- SSL.com SHALL ensure the practices and procedures of delegated parties are in compliance with S/MIME Baseline Requirements and the relevant CP and/or CPS, including the SSL.com CP/CPS. SSL.com SHALL document the obligations of delegated parties and perform monitoring on at least an annual basis of the delegated parties' adherence with those obligations.

8.4.2 Signing Service assessment

For Audit Periods starting after June 30, 2024, the Signing Service MUST undergo a conformity assessment audit for compliance with the "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates" performed in accordance with one of the following schemes:

1. "WebTrust for Certification Authorities - Code Signing Baseline Requirements v2.0 or newer" AND "WebTrust for Certification Authorities - Network Security - Version 1.0 or newer"; or
2. ETSI EN 319 411-1, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied).

Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Auditor, as specified in §8.2.

8.4.3 Timestamp Authority assessment

The Timestamp Authority MUST undergo a conformity assessment audit for compliance with the "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates" performed in accordance with one of the following schemes:

1. “WebTrust for Certification Authorities - Code Signing Baseline Requirements v2.0 or newer” AND “WebTrust for Certification Authorities - Network Security - Version 1.0 or newer”; or
2. ETSI EN 319 411-1, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied).

Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Auditor, as specified in §8.2.

8.5 Actions taken as a result of deficiency

SSL.com shall create and implement an appropriate action plan to correct any deficiency deemed to constitute material non-compliance with applicable law, the SSL.com CP/CPS, or any standard listed in §8.4.

Any corrective action plan shall be submitted to SSL.com management. Any plan which affects SSL.com policy shall also be referred to the SSL.com Policy Management Authority (PMA). Any plan shall also be communicated to any appropriate party legally obligated to be notified. Any corrective actions deemed necessary shall be implemented and documented. Corrective actions which result in changes to SSL.com policies or procedures shall be documented and incorporated into any subsequent SSL.com PKI CP/CPS.

8.6 Communication of results

Audit results are communicated to SSL.com management, the SSL.com PMA and to any third party entities entitled or required to be notified of audit results by law, regulation, or agreement. Audit compliance will be communicated to other interested parties (such as Application Service Suppliers and browser vendors) as appropriate. SSL.com makes letters showing compliance with annual external Audit Reports publicly available in the legal Repository (https://www.ssl.com/repository).

8.7 Self-Audits

SSL.com performs regular internal audits (on at least a quarterly basis) drawing upon populations of Certificates issued since the last internal audit. These audits MUST be drawn against randomly selected samples of each of the following populations:

- DV TLS Certificates;
- OV TLS Certificates;
- EV TLS Certificates;
- Code Signing Certificates;
- S/MIME Certificates;
- Document Signing Certificates; and

- Mark Certificates.

For each population, samples will consist of at least the greater of one (1) certificate or three percent (3%) of issued Certificates.

For EV TLS Certificates or for Code Signing Certificates where the Final Cross-Correlation and Due Diligence requirements of Section 3.2.2.13 of the EV Guidelines or Section 3.2.9 of the Code Signing Baseline Requirements respectively, is performed by a Delegated Third Party RA, SSL.com MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least six percent (6%) of the EV TLS or Code Signing Certificates it has issued in the period beginning immediately after the last sample was taken.

Effective 2025-03-15, SSL.com SHOULD use a Linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous linting performed on the same Certificates.

Self-audits are performed in accordance with applicable CA/B Forum Guidelines.

SSL.com shall perform an annual self-assessment evaluating the conformance of this CP/CPS against CA/B Forum Baseline Requirements and the applicable Root Program Policies.

Completed self-assessments shall be submitted to the CCADB within 92 days from the “BR Audit Period End Date” field specified in the root CA’s “CA Owner/Certificate” CCADB record (i.e. End Date of the Audit Period). If a self-assessment covers multiple CAs operating under this CP/CPS, SSL.com shall enumerate the CAs in the scope of the assessment on the provided cover sheet.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

All fees are made clear to Applicants during the enrollment process through a web interface and/or in any marketing content presented by SSL.com.

9.1.2 Certificate access fees

SSL.com reserves the right to charge for access to any database that stores information corresponding to issued Certificates.

9.1.3 Revocation or status information access fees

SSL.com may charge Subscribers who decide not to use current OCSP responders or similar systems.

9.1.4 Fees for other services

SSL.com may charge fees for additional services beyond the standard certificate procurement process.

9.1.5 Refund policy

SSL.com's Subscriber Agreement at https://www.ssl.com/repository/ includes information regarding the refund policy for all Subscribers.

9.2 Financial responsibility

9.2.1 Insurance coverage

SSL.com maintains commercial general liability insurance with policy limits of at least two million US dollars ($2,000,000) in coverage and Errors and Omissions/Professional Liability insurance with a policy limit of at least five million US dollars ($5,000,000) in coverage. SSL.com's insurance policies include coverage for

1. claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and
2. claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, patent, and trademark infringement), invasion of privacy, and advertising injury.

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

SSL.com's Subscriber Agreement at https://www.ssl.com/repository/ includes information regarding limited warranties extended to Subscribers.

9.3 Confidentiality of business information

9.3.1 Scope of Confidential Information

SSL.com classifies the following items as confidential information subject to requirements of reasonable care for protection from disclosure and misuse:

- Private Keys
- Any data regarding access to or activation of Private Keys

- Any data utilized to access the SSL.com PKI infrastructure, other than that made available to Subscribers per the SSL.com Subscriber Agreement and related agreements
- SSL.com's business continuity plans, including incident response, contingency and disaster recovery plans
- SSL.com's security documentation, including security practices and methodology
- Any data designated as private information per §9.4
- Audit logs and archive records related to any part of the SSL.com PKI
- SSL.com's transaction records, financial audit records and external or internal audit trail records related to SSL.com
- External auditor reports related to SSL.com, except for any auditor's letter or document designed for public release and confirming the results of that external audit

9.3.2 Information Not Within the Scope of Confidential Information

Any information not defined as confidential in §9.3.1 shall be deemed public. Certificate status information and Certificates issued via the SSL.com PKI are also deemed public.

9.3.3 Responsibility to Protect Confidential Information

SSL.com and all employees, agents and contractors thereof are responsible for protecting confidential information. SSL.com shall maintain and protect confidential information through thorough training and enforcement programs for all personnel.

9.4 Privacy of personal information

9.4.1 Privacy plan

All personal information utilized by any element of the SSL.com PKI is protected in accordance with SSL.com's Privacy Policy. The Privacy Policy is published at https://www.ssl.com/privacy-policy.

9.4.2 Information treated as private

All personally identifiable information received from certificate Applicants that is not ordinarily placed into a Certificate is considered private.

In accordance with §5.3, SSL.com shall train and periodically retrain all personnel to ensure secure handling of and access to private information.

9.4.3 Information not deemed private

Information contained in Certificates, certificate signing requests, or certificate revocation lists is not considered private. Any official document published to the SSL.com Repository (https://www.ssl.com/repository) is not considered private.

9.4.4 Responsibility to protect private information

All SSL.com personnel are subject to policies and confidentiality agreements that require them to handle private information in accordance with the SSL.com Privacy Policy.

9.4.5 Notice and consent to use private information

SSL.com complies with its Privacy Policy as to use of personal information, including any notice and consent requirements stated in the Privacy Policy.

In addition to permissions, consent must be specifically granted from an Applicant or Subscriber before seeking any additional information from third parties that may be required for an SSL.com product, service or operation.

9.4.6 Disclosure pursuant to judicial or administrative process

SSL.com may disclose private information without notice to Applicants or Subscribers when required to do so by law or regulation.

9.4.7 Other information disclosure circumstances

If SSL.com requires information from a third party to provide a product or service, it will obtain the Applicant's consent before seeking the information from the third party.

9.5 Intellectual property rights

SSL.com owns the intellectual property rights in SSL.com's services, and does not knowingly violate the intellectual property rights of third parties.

SSL.com retains ownership of all Certificates issued through the SSL.com PKI and associated revocation information. However, SSL.com grants permission to reproduce and distribute Certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full.

Public and Private Keys remain the property of Subscribers who legitimately hold them. All SSL.com CA Private Keys are the property of SSL.com.

9.6 Representations and warranties

9.6.1 CA representations and warranties

By issuing a Certificate, SSL.com makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;

2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate.

SSL.com represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, SSL.com has complied with its CP/CPS in issuing and managing the Certificate.

For TLS server Certificates, the Certificate Warranties specifically include, but are not limited to, the following:

1. **Right to Use Domain Name or IP Address:** That, at the time of issuance, SSL.com
    a. implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control);
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in SSL.com's Certificate Policy and/or Certification Practice Statement;
2. **Authorization for Certificate:** That, at the time of issuance, SSL.com
    a. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in SSL.com's CP/CPS;
3. **Accuracy of Information:** That, at the time of issuance, SSL.com
    a. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate;
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in SSL.com's CP/CPS;
4. **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, SSL.com
    a. implemented a procedure to verify the identity of the Applicant in accordance with §3.2;
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in SSL.com's CP/CPS;
5. **Subscriber Agreement:** That, if SSL.com and Subscriber are not Affiliated, the Subscriber and SSL.com are parties to a legally valid and enforceable Subscriber Agreement that satisfies the requirements of this CP/CPS, or, if SSL.com and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;

6. **Status:** That SSL.com maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
7. **Revocation:** That SSL.com will revoke the Certificate for any of the reasons specified in this CP/CPS.

SSL.com shall be responsible for the performance and warranties of the Subordinate CAs and for all liabilities and indemnification obligations of the Subordinate CAs under this CP/CPS.

For Extended Validation Certificates, the EV Certificate Warranties specifically include, but are not limited to, the following:

1. **Legal Existence:** SSL.com has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
2. **Identity:** SSL.com has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
3. **Right to Use Domain Name:** For TLS server Certificates SSL.com has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the right to use all the Domain Name(s) listed in the EV Certificate;
4. **Authorization for EV Certificate:** SSL.com has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;
5. **Accuracy of Information:** SSL.com has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;
6. **Subscriber Agreement:** The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with SSL.com that satisfies the requirements of this CP/CPS or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;
7. **Status:** SSL.com will follow the procedures of this CP/CPS and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and
8. **Revocation:** SSL.com will follow the procedures of this CP/CPS and revoke the EV Certificate for any of the revocation reasons specified in this CP/CPS.

For Code Signing Certificates,

1. **Compliance:** SSL.com and any Delegated Third Party each represents that it has complied with these Requirements and the applicable Certificate Policy and Certification

Practice Statement in issuing each Code Signing Certificate and operating its PKI or delegated service.

2. **Identity of Applicant:** At the time of issuance, the CA represents that it:
    a. operated a procedure for verifying the identity of the Subscriber that at least meets the requirements in §3.2 of this document;
    b. followed the procedure when issuing or managing the Certificate; and
    c. accurately described the procedure in SSL.com's CP/CPS;
3. **Authorization for Certificate:** That, at the time of issuance, SSL.com
    a. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in SSL.com's CP/CPS;
4. **Accuracy of Information:** That, at the time of issuance, SSL.com
    a. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the `subject:organizationalUnitName` attribute)
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in SSL.com's CP/CPS;
5. **Key Protection:** The Issuer represents that it provided the Subscriber at the time of issuance with documentation on how to securely store and prevent the misuse of Private Keys associated with Code Signing Certificates, or in the case of a Signing Service, securely stored and prevented the misuse of Private Keys associated with Code Signing Certificates;
6. **Subscriber Agreement:** That, if SSL.com and Subscriber are not Affiliated, the Subscriber and SSL.com are parties to a legally valid and enforceable Subscriber Agreement that satisfies the requirements of this CP/CPS, or, if SSL.com and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
7. **Status:** SSL.com represents that it will maintain a 24 x 7 online-accessible Repository with current information regarding the status of Code Signing Certificates as valid or revoked for the period required by this CP/CPS; and
8. **Revocation:** That SSL.com will revoke the Certificate for any of the reasons specified in this CP/CPS.

9.6.2 RA representations and warranties

Any Registration Authority (RA) utilizing SSL.com's PKI shall warrant that:

1. All certificate management operations conform to the SSL.com CP/CPS and any other related or relevant documents.
2. Information provided by the RA does not contain any false or misleading information.
3. Any translations provided by the RA are accurate.

4. Any RA shall abide by the terms of any Registration Authority Agreement (RAA) signed with SSL.com.

Additional RA-specific contractual stipulations may apply.

9.6.3 Subscriber representations and warranties

SSL.com shall require each Applicant to enter into a Subscription Agreement that is legally enforceable against the Applicant/Subscriber and covers each Certificate request and resulting Certificate. The Subscription Agreement shall include the following commitments and warranties by the Subscriber for the benefit of SSL.com and the Certificate Beneficiaries:

1. **Accuracy of Information:** all information provided by the Applicant/Subscriber is accurate, complete, and up to date, both in the Certificate request and as otherwise requested by SSL.com in connection with the issuance of the Certificate(s) to be supplied by SSL.com;
2. **Protection of Private Key:** Subscriber shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token); Where the key is available outside a Signing Service, to maintain sole control of, keep confidential, and properly protect, at all times in accordance with §4.5.1, the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token). SSL.com MUST provide the Subscriber with documentation on how to protect a Private Key. SSL.com MAY provide this documentation as a white paper or as part of the Subscriber Agreement. The Subscriber MUST represent that it will generate and operate any device storing private keys in a secure manner, as described in a document of Code Signing best practices, which SSL.com MUST provide to the Subscriber during the ordering process. SSL.com MUST obligate the Subscriber to use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.
3. **Prevention of Misuse:** For Code Signing and EV Code Signing Certificates, Subscriber has an obligation to provide adequate network and other security controls to protect against misuse of the Private Key and that SSL.com will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys
4. **Private Key Reuse:** Subscriber has an obligation to not apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate
5. **Acceptance of Certificate:** Subscriber will review and verify the Certificate contents for accuracy;
6. **Use of Certificate:** Subscriber shall install and use the Certificate solely in compliance with all applicable laws, solely in accordance with the Subscriber Agreement and solely for the purposes it was intended to be used for. For Code Signing and EV Code Signing

Certificates, the Subscriber shall not knowingly sign software that contains Suspect Code and use the Code Signing and EV Code Signing Certificate as follows:

   a. only to sign code that complies with the requirements set forth in the Code Signing Baseline Requirements;
   b. solely in compliance with all applicable laws;
   c. solely for authorized company business; and
   d. solely in accordance with the Subscriber Agreement;

7. **Reporting and Revocation:** Subscriber has an obligation and warranty to:
   a. promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate,
   b. promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate, and
   c. for Code Signing and EV Code Signing Certificates, promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is evidence that the certificate was used to sign Suspect Code;
   d. for Server Certificates, when requesting revocation of the Certificate, report the most relevant revocation reason per §4.9.1.1;
8. **Termination of Use of Certificate:** Subscriber has an obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon expiration or revocation of that Certificate;
9. **Responsiveness:** Subscriber has an obligation to respond to SSL.com's instructions concerning Key Compromise or Certificate misuse within a specified time period;
10. **Acknowledgment and Acceptance:** Subscriber acknowledges and accepts that SSL.com is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or if revocation is required by SSL.com's CP/CPS, or if SSL.com discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4 Relying party representations and warranties

A Relying Party utilizing any certificate created using SSL.com's PKI makes the following warranties and commitments in a Relying Party Agreement:

1. It shall verify that any third party issuing a Certificate is an authorized subordinate Certification Authority of SSL.com and that the Certificate was issued in accordance with the policies set out in SSL.com's CP/CPS;
2. It shall check the CRL/OSCP to ensure that the Certificate is valid and not revoked or terminated;
3. It acknowledges that SSL.com performs differing degrees of Certificate validation depending on the type of Certificate and intended use, and that it must take those factors into consideration when deciding whether or not to rely on a Certificate;

4. It complies with all applicable policies and procedures set out in the SSL.com CP/CPS, including, without limitation, a requirement that the Certificate not be used for any purpose other than as set forth in the relevant section of this CP/CPS for the particular class and type of Certificate.

A copy of the latest SSL.com Certificate Relying Party Agreement and SSL.com Relying Party Warranty are available in the SSL.com repository at https://www.ssl.com/relying-party-agreement and https://www.ssl.com/relying-party-warranty, respectively.

9.6.5 Representations and warranties of other participants

SSL.com SHALL contractually obligate each Signing Service to inform SSL.com if the Signing Service becomes aware (by whatever means) that the Signing Service has signed Suspect Code. SSL.com SHALL require the Signing Service to request revocation of the affected Certificate and provide immediate notice to SSL.com if the Subscriber's Private Key, or Private Key activation data, is compromised or believed to be compromised. SSL.com SHALL revoke the affected Certificate upon request by the Signing Service or if SSL.com determines the Signing Service failed to notify SSL.com within 24 hours after identifying a Key Compromise.

Signing Services SHALL obtain the Subscriber's commitment to:

1. Use such signing services solely for authorized purposes that comply with the Subscriber Agreement/Terms of Use, these Requirements, and all applicable laws,
2. Not knowingly submit software for Code Signature that contains Suspect Code, and
3. Inform the Signing Service if it is discovered (by whatever means) that Code submitted to the Signing Service for Code Signature contained Suspect Code

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, SSL.COM DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

SSL.COM DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE.

SSL.com does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

SSL.com does not guarantee the accuracy, authenticity, completeness or fitness of any information contained in test or demo Certificates, such as Test Document Signing Certificates.

No fiduciary duty is created or implied though use of SSL.com services by any entity.

9.8 Limitations of liability

For delegated tasks, SSL.com and any Delegated Third Party may allocate liability between themselves contractually as they determine, but SSL.com shall remain fully responsible for the performance of all parties in accordance with this CP/CPS, as if the tasks had not been delegated.

If SSL.com has issued and managed the Certificate in compliance with this CP/CPS, SSL.com may disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in SSL.com's CP/CPS. If SSL.com has not issued or managed the Certificate in compliance with its CP/CPS, SSL.com may seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that SSL.com desires. If SSL.com chooses to limit its liability for Certificates that are not issued or managed in compliance with its CP/CPS, then SSL.com shall include the limitations on liability in SSL.com's CP/CPS.

SSL.com MAY NOT limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than two thousand (2,000) US dollars per Subscriber or Relying Party per Mark Certificate.

In no event is SSL.com liable for any losses or damages suffered as a result of use or reliance on test or demo Certificates, such as Test Document Signing Certificates.

9.9 Indemnities

9.9.1 Indemnification by CAs

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, SSL.com understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of SSL.com under this CP/CPS or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, SSL.com shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by SSL.com, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by SSL.com where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy:

1. a Certificate that has expired, or
2. a Certificate that has been revoked (but only in cases where the revocation status is currently available from SSL.com online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify SSL.com, 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

1. any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional;
2. Subscriber's breach of the Subscriber Agreement, this CP/CPS, or applicable law;
3. the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence or intentional acts; or
4. Subscriber's misuse of the certificate or Private Key.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify SSL.com, 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 the Relying Party's

1. breach of the Relying Party Agreement, an End-User License Agreement, this CP/CPS, or applicable law;
2. unreasonable reliance on a certificate; or
3. failure to check the certificate's status prior to use.

9.10 Term and termination

9.10.1 Term

This version of the SSL.com CP/CPS is effective until otherwise communicated through the SSL.com repository. (https://www.ssl.com/repository)

9.10.2 Termination

The termination of any SSL.com CP/CPS becomes effective immediately following the publication of a more recent version. Some sections of the CP/CPS may include specific future dates after which certain policies or practices will become effective.

9.10.3 Effect of termination and survival

SSL.com will publicly communicate any CA termination through its public repository and the Application Software Suppliers who have a Root Certificate distribution agreement in place with SSL.com.

9.11 Individual notices and communications with participants

SSL.com accepts forms of notice related to this CP/CPS which either implement a digital signature or employ a physical mail service. Paper forms of notice must be delivered with a courier service that confirms delivery or via certified mail. Only digitally signed messages of notice that are judged to be valid shall receive an SSL.com response. SSL.com contact information for notices using certified mail is provided in §1.5.2. Valid communications will be reviewed and replied to as appropriate in a timely manner.

9.12 Amendments

9.12.1 Procedure for amendment

SSL.com's Policy Management Authority (PMA) may enact amendments to this CP/CPS as required.

Any significant changes made to the SSL.com CP/CPS shall be noted in a version control table incorporated into this CP/CPS.

Minor changes (e.g. correction of grammatical, syntactical, spelling errors) may, at SSL.com's sole discretion, be carried out without any prior notice and by adding a sub-minor number in the document OID.

On an annual basis, if no other changes are made to the document, its version number shall be incremented and a dated changelog entry shall be added to denote that.

9.12.2 Notification mechanism and period

SSL.com shall upload updated versions of this CP/CPS to its legal Repository and the CCADB within 7 days of being updated.

Subscribers shall be duly notified in case of major changes to this CP/CPS, especially in regards to any specific effective dates that enable policy and procedural changes.

9.12.3 Circumstances under which OID must be changed

SSL.com reserves the right to amend content of any published CP/CPS. Any major change of the SSL.com CP/CPS will also alter the OID of the CP/CPS published via the SSL.com repository.

9.13 Dispute resolution provisions

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

9.14 Governing law

The laws of the state of Texas govern the interpretation, construction, and enforcement of this CP/CPS and all proceedings related to SSL.com's products and services, including tort claims, without regard to any conflicts of law principles. The state of Texas has non-exclusive venue and jurisdiction over any proceedings related to this CP/CPS or any SSL.com product or service.

9.15 Compliance with applicable law

This CP/CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products.

Subject to §9.4.5's Notice and Consent to Use Private Information contained in Certificates, SSL.com meets the requirements of the European data protection laws and has established appropriate technical and organization measures 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

SSL.com contractually obligates each RA to comply with this CP/CPS and applicable industry guidelines. SSL.com also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CP/CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

Any entities operating under this CP/CPS may not assign their rights or obligations without the prior written consent of SSL.com. Unless specified otherwise in a contact with a party, SSL.com does not provide notice of assignment.

9.16.3 Severability

In the event of a conflict between the SSL.com CP/CPS and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which SSL.com operates or issues certificates, SSL.com MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction.

This applies only to operations or certificate issuances that are subject to that Law.

In such event, SSL.com SHALL immediately (and prior to issuing a certificate under the modified requirement) include in §9.16.3 of this CP/CPS a detailed reference to the Law requiring a modification of this CP/CPS under this section, and the specific modifications to the CP/CPS as implemented by SSL.com.

SSL.com MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum or the AuthIndicators Working Group of the relevant information newly added to its CPS by sending a message to to the applicable mailing list and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives (or such other email addresses and links as the Forum or AuthIndicators Working Group may designate), so that the CA/Browser Forum or AuthIndicators Working Group may consider possible revisions to the corresponding standards accordingly.

Any modification to CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or the CA/Browser Forum Baseline Requirements (and therefore the SSL.com CP/CPS) are modified to make it possible to comply with both them and the Law simultaneously without reliance on specific modifications within 9.16.3.

An appropriate change in practice, modification to SSL.com's CP/CPS and a notice to the CA/Browser Forum, as outlined above, must be made within 90 days from the date the law becomes effective as to SSL.com.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

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

9.16.5 Force Majeure

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

9.17 Other provisions

No stipulation

ANNEX A - SSL.com Commonly used Certificate Profiles

Friendly Name	Policy IDs	Key Usages	Other Extensions
SSL.com Intermediate CA Certificate	**2.5.29.32.0 (anyPolicy)**	*KU:* Certificate Signing, CRL Signing, Digital Signature (optional) *EKU:* (Optional) Depending on the Intermediate CA Certificate usage	None

Friendly Name	Policy IDs	Key Usages	Other Extensions
OCSP Responder Certificate	**1.3.6.1.4.1.38064.1.3.7**	*KU:* Digital Signature *EKU:* **OCSP Signing** (`1.3.6.1.5.5.7.3.9`)	**OCSP No Check**
SSL DV	**2.23.140.1.2.1**, **1.3.6.1.4.1.38064.1.3.1.1**	*KU:* Digital Signature, Key Encipherment[4] *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`), **TLS Web Server Authentication** (`1.3.6.1.5.5.7.3.1`)	None
SSL OV	**2.23.140.1.2.2**, **1.3.6.1.4.1.38064.1.3.1.2**	*KU:* Digital Signature, Key Encipherment[5] *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`), **TLS Web Server Authentication** (`1.3.6.1.5.5.7.3.1`)	None
SSL IV	**2.23.140.1.2.3**, **1.3.6.1.4.1.38064.1.3.1.3**	*KU:* Digital Signature, Key Encipherment[6] *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`), **TLS Web Server Authentication** (`1.3.6.1.5.5.7.3.1`)	None

[4] **"Key Encipherment"** is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

[5] **"Key Encipherment"** is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

[6] **"Key Encipherment"** is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

Friendly Name	Policy IDs	Key Usages	Other Extensions
SSL EV	**2.23.140.1.1**, **1.2.616.1.113527.2.5.1.1**, **1.3.6.1.4.1.38064.1.3.1.4**	*KU:* Digital Signature, Key Encipherment[7] *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`), **TLS Web Server Authentication** (`1.3.6.1.5.5.7.3.1`)	None
S/MIME email only (SMIME/Client) - Generation: Multipurpose	**2.23.140.1.5.1.2, 1.3.6.1.4.1.38064.1.3.2.1, 1.3.6.1.4.1.38064.1.3.5.7**	*KU:* Digital Signature, Key Encipherment[8] *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`), **Email Protection** (`1.3.6.1.5.5.7.3.4`)	None
S/MIME OV (SMIME/Client) - Generation: Multipurpose	**2.23.140.1.5.2.2, 1.3.6.1.4.1.38064.1.3.2.2, 1.3.6.1.4.1.38064.1.3.5.1**	*KU:* Digital Signature, Key Encipherment[9] *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`), **Email Protection** (`1.3.6.1.5.5.7.3.4`)	None
S/MIME SV, i.e. OV plus IV (SMIME/Client) - Generation: Multipurpose	**2.23.140.1.5.3.2, 1.3.6.1.4.1.38064.1.3.2.2, 1.3.6.1.4.1.38064.1.3.5.1**	*KU:* Digital Signature, Key Encipherment[10] *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`), **Email Protection** (`1.3.6.1.5.5.7.3.4`)	None

[7] **"Key Encipherment"** is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

[8] **"Key Encipherment"** is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

[9] **"Key Encipherment"** is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

[10] **"Key Encipherment"** is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

Friendly Name	Policy IDs	Key Usages	Other Extensions
S/MIME IV (SMIME/Client) - Generation: Multipurpose	**2.23.140.1.5.4.2, 1.3.6.1.4.1.38064.1.3.2.3, 1.3.6.1.4.1.38064.1.3.5.2**	*KU:* Digital Signature, Key Encipherment[11] *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`), **Email Protection** (`1.3.6.1.5.5.7.3.4`)	None
Document Signing OV (Client/docSigning)	**1.3.6.1.4.1.38064.1.3.4.1**, **1.3.6.1.4.1.38064.1.3.5.1**	*KU:* Digital Signature, Non Repudiation *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`), **Document Signing** (`1.3.6.1.5.5.7.3.36`), **msDocSigning** (1.3.6.1.4.1.311.10.3.12), **AuthenticDocumentsTrust** (`1.2.840.113583.1.1.5`)	None
Document Signing IV (Client/docSigning)	**1.3.6.1.4.1.38064.1.3.4.2**, **1.3.6.1.4.1.38064.1.3.5.2**	*KU:* Digital Signature, Non Repudiation *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`), **Document Signing** (`1.3.6.1.5.5.7.3.36`), **msDocSigning** (1.3.6.1.4.1.311.10.3.12), **AuthenticDocumentsTrust** (`1.2.840.113583.1.1.5`)	None

[11] **"Key Encipherment"** is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

Friendly Name	Policy IDs	Key Usages	Other Extensions
Code Signing	**2.23.140.1.4.1**, **1.3.6.1.4.1.38064.1.3.3.1**	*KU:* Digital Signature *EKU:* **Code Signing** (`1.3.6.1.5.5.7.3.3`)	None
Code Signing with Lifetime Signing	**2.23.140.1.4.1**, **1.3.6.1.4.1.38064.1.3.3.1**	*KU:* Digital Signature *EKU:* **Code Signing** (`1.3.6.1.5.5.7.3.3`), **Lifetime Signing** (`1.3.6.1.4.1.311.10.3.13`)	None
EV Code Signing	**2.23.140.1.3**, **1.2.616.1.113527.2.5.1.7**, **1.3.6.1.4.1.38064.1.3.3.2**	*KU:* Digital Signature *EKU:* **Code Signing** (`1.3.6.1.5.5.7.3.3`)	None
EV Code Signing with Lifetime Signing	**2.23.140.1.3**, **1.2.616.1.113527.2.5.1.7**, **1.3.6.1.4.1.38064.1.3.3.2**	*KU:* Digital Signature *EKU:* **Code Signing** (`1.3.6.1.5.5.7.3.3`), **Lifetime Signing** (`1.3.6.1.4.1.311.10.3.13`)	None
Basic Time-stamping	**1.3.6.1.4.1.38064.1.3.6.1**, **2.23.140.1.4.2**	*KU:* Digital Signature *EKU:* **TimeStamping** (`1.3.6.1.5.5.7.3.8`)	None
EV Time-stamping	**1.3.6.1.4.1.38064.1.3.6.2**, **2.23.140.1.4.2**	*KU:* Digital Signature *EKU:* **TimeStamping** (`1.3.6.1.5.5.7.3.8`)	None
Time-stamping Certificate for Document Signing Trust	**1.3.6.1.4.1.38064.1.3.6.3**	*KU:* Digital Signature *EKU:* **TimeStamping** (`1.3.6.1.5.5.7.3.8`)	None
NAESB Client Cert Rudimentary Assurance	**2.16.840.1.114505.1.12.1.2**, **1.3.6.1.4.1.38064.1.3.5.3**	*KU:* Digital Signature *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`)	None
NAESB Client Cert Basic Assurance	**2.16.840.1.114505.1.12.2.2**, **1.3.6.1.4.1.38064.1.3.5.4**	*KU:* Digital Signature *EKU:* **TLS Web Client Authentication** (`1.3.6.1.5.5.7.3.2`)	None
NAESB Client Cert Medium Assurance	**2.16.840.1.114505.1.12.3.2**, **1.3.6.1.4.1.38064.1.3.5.5**	*KU:* Digital Signature *EKU:* **TLS Web Client**	None

Friendly Name	Policy IDs	Key Usages	Other Extensions
		Authentication (1.3.6.1.5.5.7.3.2)	
NAESB Client Cert High Assurance	**2.16.840.1.114505.1.12.4.2**, **1.3.6.1.4.1.38064.1.3.5.6**	*KU:* Digital Signature *EKU:* **TLS Web Client Authentication** (1.3.6.1.5.5.7.3.2)	None
NAESB Server Cert Basic Assurance	**2.23.140.1.2.2**, **2.16.840.1.114505.1.12.2.2**, **1.3.6.1.4.1.38064.1.3.1.5**	*KU:* Digital Signature, Key Encipherment[12] *EKU:* **TLS Web Client Authentication** (1.3.6.1.5.5.7.3.2), **TLS Web Server Authentication** (1.3.6.1.5.5.7.3.1)	None
NAESB Server Cert Medium Assurance	**2.23.140.1.1**, **2.16.840.1.114505.1.12.3.2**, **1.3.6.1.4.1.38064.1.3.1.6**	*KU:* Digital Signature, Key Encipherment[13] *EKU:* **TLS Web Client Authentication** (1.3.6.1.5.5.7.3.2), **TLS Web Server Authentication** (1.3.6.1.5.5.7.3.1)	None

[12] **"Key Encipherment"** is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

[13] **"Key Encipherment"** is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.