Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates

Version 2.3.1 modified with changes from ballot SC105 that passed the Initial Vote, for Review Notice purposes only (not yet in effect).

CA/Browser Forum

4-Oct-2026

Table of Contents

1. INTRODUCTION 11
   1.1 Overview 11
   1.2 Document name and identification 12
      1.2.1 Revisions 12
      1.2.2 Relevant Dates 17
   1.3 PKI Participants 19
      1.3.1 Certification Authorities 19
      1.3.2 Registration Authorities 19
      1.3.3 Subscribers 20
      1.3.4 Relying Parties 20
      1.3.5 Other Participants 20
   1.4 Certificate Usage 21
      1.4.1 Appropriate Certificate Uses 21
      1.4.2 Prohibited Certificate Uses 21
   1.5 Policy administration 21
      1.5.1 Organization Administering the Document 21
      1.5.2 Contact Person 21
      1.5.3 Person Determining CPS suitability for the policy 21
      1.5.4 CPS approval procedures 21
   1.6 Definitions and Acronyms 22
      1.6.1 Definitions 22
      1.6.2 Acronyms 31
      1.6.3 References 32
      1.6.4 Conventions 35
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 36
   2.1 Repositories 36
   2.2 Publication of information 36
   2.3 Time or frequency of publication 36
   2.4 Access controls on repositories 37
3. IDENTIFICATION AND AUTHENTICATION 38
   3.1 Naming 38

DRAFT

3.1.1 Types of names 38
3.1.2 Need for names to be meaningful 38
3.1.3 Anonymity or pseudonymity of subscribers 38
3.1.4 Rules for interpreting various name forms 38
3.1.5 Uniqueness of names 38
3.1.6 Recognition, authentication, and role of trademarks 38
3.2 Initial identity validation 38
3.2.1 Method to prove possession of private key 38
3.2.2 Authentication of Organization and Domain Identity 38
3.2.3 Authentication of individual identity 59
3.2.4 Non-verified subscriber information 59
3.2.5 Validation of authority 59
3.2.6 Criteria for Interoperation or Certification 60
3.3 Identification and authentication for re-key requests 60
3.3.1 Identification and authentication for routine re-key 60
3.3.2 Identification and authentication for re-key after revocation 60
3.4 Identification and authentication for revocation request 60
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 61
4.1 Certificate Application 61
4.1.1 Who can submit a certificate application 61
4.1.2 Enrollment process and responsibilities 61
4.2 Certificate application processing 61
4.2.1 Performing identification and authentication functions 61
4.2.2 Approval or rejection of certificate applications 63
4.2.3 Time to process certificate applications 66
4.3 Certificate issuance 67
4.3.1 CA actions during certificate issuance 67
4.3.2 Notification to subscriber by the CA of issuance of certificate 68
4.4 Certificate acceptance 68
4.4.1 Conduct constituting certificate acceptance 68
4.4.2 Publication of the certificate by the CA 68
4.4.3 Notification of certificate issuance by the CA to other entities 68

DRAFT

4.5 Key pair and certificate usage 68
4.5.1 Subscriber private key and certificate usage 68
4.5.2 Relying party public key and certificate usage 68
4.6 Certificate renewal 68
4.6.1 Circumstance for certificate renewal 68
4.6.2 Who may request renewal 68
4.6.3 Processing certificate renewal requests 68
4.6.4 Notification of new certificate issuance to subscriber 68
4.6.5 Conduct constituting acceptance of a renewal certificate 69
4.6.6 Publication of the renewal certificate by the CA 69
4.6.7 Notification of certificate issuance by the CA to other entities 69
4.7 Certificate re-key 69
4.7.1 Circumstance for certificate re-key 69
4.7.2 Who may request certification of a new public key 69
4.7.3 Processing certificate re-keying requests 69
4.7.4 Notification of new certificate issuance to subscriber 69
4.7.5 Conduct constituting acceptance of a re-keyed certificate 69
4.7.6 Publication of the re-keyed certificate by the CA 69
4.7.7 Notification of certificate issuance by the CA to other entities 69
4.8 Certificate modification 69
4.8.1 Circumstance for certificate modification 69
4.8.2 Who may request certificate modification 70
4.8.3 Processing certificate modification requests 70
4.8.4 Notification of new certificate issuance to subscriber 70
4.8.5 Conduct constituting acceptance of modified certificate 70
4.8.6 Publication of the modified certificate by the CA 70
4.8.7 Notification of certificate issuance by the CA to other entities 70
4.9 Certificate revocation and suspension 70
4.9.1 Circumstances for revocation 70
4.9.2 Who can request revocation 72
4.9.3 Procedure for revocation request 72
4.9.4 Revocation request grace period 72

DRAFT

4.9.5 Time within which CA must process the revocation request 73
4.9.6 Revocation checking requirement for relying parties 73
4.9.7 CRL issuance frequency 73
4.9.8 Maximum latency for CRLs (if applicable) 74
4.9.9 On-line revocation/status checking availability 74
4.9.10 On-line revocation checking requirements 75
4.9.11 Other forms of revocation advertisements available 75
4.9.12 Special requirements re key compromise 75
4.9.13 Circumstances for suspension 76
4.9.14 Who can request suspension 76
4.9.15 Procedure for suspension request 76
4.9.16 Limits on suspension period 76
4.10 Certificate status services 76
4.10.1 Operational characteristics 76
4.10.2 Service availability 76
4.10.3 Optional features 76
4.11 End of subscription 76
4.12 Key escrow and recovery 77
4.12.1 Key escrow and recovery policy and practices 77
4.12.2 Session key encapsulation and recovery policy and practices 77
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS 78
5.1 Physical Security Controls 79
5.1.1 Site location and construction 79
5.1.2 Physical access 79
5.1.3 Power and air conditioning 79
5.1.4 Water exposures 79
5.1.5 Fire prevention and protection 79
5.1.6 Media storage 79
5.1.7 Waste disposal 79
5.1.8 Off-site backup 79
5.2 Procedural controls 79
5.2.1 Trusted roles 79

DRAFT

5.2.2 Number of Individuals Required per Task 79
5.2.3 Identification and authentication for each role 79
5.2.4 Roles requiring separation of duties 79
5.3 Personnel controls 79
5.3.1 Qualifications, experience, and clearance requirements 79
5.3.2 Background check procedures 80
5.3.3 Training Requirements and Procedures 80
5.3.4 Retraining frequency and requirements 80
5.3.5 Job rotation frequency and sequence 80
5.3.6 Sanctions for unauthorized actions 80
5.3.7 Independent Contractor Controls 80
5.3.8 Documentation supplied to personnel 80
5.4 Audit logging procedures 80
5.4.1 Types of events recorded 80
5.4.2 Frequency of processing audit log 82
5.4.3 Retention period for audit log 82
5.4.4 Protection of audit log 83
5.4.5 Audit log backup procedures 83
5.4.6 Audit collection System (internal vs. external) 83
5.4.7 Notification to event-causing subject 83
5.4.8 Vulnerability assessments 83
5.5 Records archival 83
5.5.1 Types of records archived 83
5.5.2 Retention period for archive 83
5.5.3 Protection of archive 84
5.5.4 Archive backup procedures 84
5.5.5 Requirements for time-stamping of records 84
5.5.6 Archive collection system (internal or external) 84
5.5.7 Procedures to obtain and verify archive information 84
5.6 Key changeover 84
5.7 Compromise and disaster recovery 84
5.7.1 Incident and compromise handling procedures 84

DRAFT

5.7.2 Recovery Procedures if Computing resources, software, and/or data are corrupted 86
5.7.3 Recovery Procedures after Key Compromise 86
5.7.4 Business continuity capabilities after a disaster 86
5.8 CA or RA termination 86
6. TECHNICAL SECURITY CONTROLS 87
6.1 Key pair generation and installation 87
6.1.1 Key pair generation 87
6.1.2 Private key delivery to subscriber 88
6.1.3 Public key delivery to certificate issuer 89
6.1.4 CA public key delivery to relying parties 89
6.1.5 Key sizes 89
6.1.6 Public key parameters generation and quality checking 89
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 89
6.2 Private Key Protection and Cryptographic Module Engineering Controls 89
6.2.1 Cryptographic module standards and controls 90
6.2.2 Private key (n out of m) multi-person control 90
6.2.3 Private key escrow 90
6.2.4 Private key backup 90
6.2.5 Private key archival 90
6.2.6 Private key transfer into or from a cryptographic module 90
6.2.7 Private key storage on cryptographic module 90
6.2.8 Activating Private Keys 91
6.2.9 Deactivating Private Keys 91
6.2.10 Destroying Private Keys 91
6.2.11 Cryptographic Module Rating 91
6.3 Other aspects of key pair management 91
6.3.1 Public key archival 91
6.3.2 Certificate operational periods and key pair usage periods 91
6.4 Activation data 92
6.4.1 Activation data generation and installation 92
6.4.2 Activation data protection 92

DRAFT

6.4.3 Other aspects of activation data 92
6.5 Computer security controls 92
6.5.1 Specific computer security technical requirements 92
6.5.2 Computer security rating 92
6.6 Life cycle technical controls 92
6.6.1 System development controls 92
6.6.2 Security management controls 92
6.6.3 Life cycle security controls 92
6.7 Network security controls 92
6.8 Time-stamping 92
7. CERTIFICATE, CRL, AND OCSP PROFILES 93
7.1 Certificate profile 93
7.1.1 Version number(s) 93
7.1.2 Certificate Content and Extensions 93
7.1.3 Algorithm object identifiers 141
7.1.4 Name Forms 144
7.1.5 Name constraints 148
7.1.6 Certificate policy object identifier 148
7.1.7 Usage of Policy Constraints extension 148
7.1.8 Policy qualifiers syntax and semantics 148
7.1.9 Processing semantics for the critical Certificate Policies extension 148
7.2 CRL profile 148
7.2.1 Version number(s) 150
7.2.2 CRL and CRL entry extensions 150
7.3 OCSP profile 153
7.3.1 Version number(s) 154
7.3.2 OCSP extensions 154
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 155
8.1 Frequency or circumstances of assessment 155
8.2 Identity/qualifications of assessor 155
8.3 Assessor's relationship to assessed entity 156
8.4 Topics covered by assessment 156

DRAFT

8.5 Actions taken as a result of deficiency 157
8.6 Communication of results 157
8.7 Self-Audits 158
9. OTHER BUSINESS AND LEGAL MATTERS 159
9.1 Fees 159
9.1.1 Certificate issuance or renewal fees 159
9.1.2 Certificate access fees 159
9.1.3 Revocation or status information access fees 159
9.1.4 Fees for other services 159
9.1.5 Refund policy 159
9.2 Financial responsibility 159
9.2.1 Insurance coverage 159
9.2.2 Other assets 159
9.2.3 Insurance or warranty coverage for end-entities 159
9.3 Confidentiality of business information 159
9.3.1 Scope of confidential information 159
9.3.2 Information not within the scope of confidential information 159
9.3.3 Responsibility to protect confidential information 159
9.4 Privacy of personal information 159
9.4.1 Privacy plan 159
9.4.2 Information treated as private 159
9.4.3 Information not deemed private 159
9.4.4 Responsibility to protect private information 159
9.4.5 Notice and consent to use private information 159
9.4.6 Disclosure pursuant to judicial or administrative process 159
9.4.7 Other information disclosure circumstances 159
9.5 Intellectual property rights 160
9.6 Representations and warranties 160
9.6.1 CA representations and warranties 160
9.6.2 RA representations and warranties 161
9.6.3 Subscriber representations and warranties 161
9.6.4 Relying party representations and warranties 163

DRAFT

9.6.5 Representations and warranties of other participants 163
9.7 Disclaimers of warranties 163
9.8 Limitations of liability 163
9.9 Indemnities 163
9.10 Term and termination 164
9.10.1 Term 164
9.10.2 Termination 164
9.10.3 Effect of termination and survival 164
9.11 Individual notices and communications with participants 164
9.12 Amendments 164
9.12.1 Procedure for amendment 164
9.12.2 Notification mechanism and period 164
9.12.3 Circumstances under which OID must be changed 164
9.13 Dispute resolution provisions 164
9.14 Governing law 164
9.15 Compliance with applicable law 164
9.16 Miscellaneous provisions 165
9.16.1 Entire agreement 165
9.16.2 Assignment 165
9.16.3 Severability 165
9.16.4 Enforcement (attorneys' fees and waiver of rights) 165
9.16.5 Force Majeure 165
9.17 Other provisions 165
Appendix A – CAA Contact Tag 166
A.1. CAA Methods 166
A.1.1. CAA contactemail Property 166
A.1.2. CAA contactphone Property 166
A.2. DNS TXT Methods 166
A.2.1. DNS TXT Record Email Contact 166
A.2.2. DNS TXT Record Phone Contact 167
Appendix B – Issuance of Certificates for Onion Domain Names 168

DRAFT

1. INTRODUCTION

1.1 Overview

This document describes an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements that are necessary (but not sufficient) for the issuance and management of Publicly-Trusted TLS Server Certificates; Certificates that are trusted by virtue of the fact that their corresponding Root Certificate is distributed in widely-available application software. The requirements are not mandatory for Certification Authorities unless and until they become adopted and enforced by relying-party Application Software Suppliers.

Notice to Readers

The CP for the Issuance and Management of Publicly-Trusted TLS Server Certificates describe a subset of the requirements that a Certification Authority must meet in order to issue Publicly Trusted TLS Server Certificates. This document serves two purposes: to specify Baseline Requirements and to provide guidance and requirements for what a CA should include in its CPS. Except where explicitly stated otherwise, these Requirements apply only to relevant events that occur on or after 2012-07-01 (the original effective date of these requirements).

These Requirements do not address all of the issues relevant to the issuance and management of Publicly-Trusted TLS Server Certificates. In accordance with RFC 3647 and to facilitate a comparison of other certificate policies and CPSs (e.g. for policy mapping), this document includes all sections of the RFC 3647 framework. However, rather than beginning with a "no stipulation" comment in all empty sections, the CA/Browser Forum is leaving such sections initially blank until a decision of "no stipulation" is made. The CA/Browser Forum may update these Requirements from time to time, in order to address both existing and emerging threats to online security. In particular, it is expected that a future version will contain more formal and comprehensive audit requirements for delegated functions.

These Requirements only address Certificates intended to be used for authenticating servers accessible through the Internet. Similar requirements for code signing, S/MIME, time-stamping, VoIP, IM, Web services, etc. may be covered in future versions.

These Requirements do not address the issuance, or management of Certificates by enterprises that operate their own Public Key Infrastructure for internal purposes only, and for which the Root Certificate is not distributed by any Application Software Supplier.

DRAFT

These Requirements are applicable to all Certification Authorities within a chain of trust. They are to be flowed down from the Root Certification Authority through successive Subordinate Certification Authorities.

1.2 Document name and identification

This certificate policy (CP) contains the requirements for the issuance and management of publicly-trusted TLS Server certificates, as adopted by the CA/Browser Forum.

The following Certificate Policy identifiers are reserved for use by CAs to assert compliance with this document (OID arc 2.23.140.1.2) as follows:

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)`; and

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

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3)`.

1.2.1 Revisions

Ver.	Ballot	Description	Adopted	Effective*
1.0.0	62	Version 1.0 of the Baseline Requirements Adopted	2011-11-22	2012-07-01
1.0.1	71	Revised Auditor Qualifications	2012-05-08	2013-01-01
1.0.2	75	Non-critical Name Constraints allowed as exception to RFC 5280	2012-06-08	2012-06-08
1.0.3	78	Revised Domain/IP Address Validation, High Risk Requests, and Data Sources	2012-06-22	2012-06-22
1.0.4	80	OCSP responses for non-issued certificates	2012-08-02	2013-08-02
–	83	Network and Certificate System Security Requirements adopted	2013-08-03	2013-01-01
1.0.5	88	User-assigned country code of XX allowed	2012-09-12	2012-09-12
1.1.0	–	Published as Version 1.1 with no changes from 1.0.5	2012-09-14	2012-09-14
1.1.1	93	Reasons for Revocation and Public Key Parameter checking	2012-11-07	2012-11-07

DRAFT

Ver.	Ballot	Description	Adopted	Effective*
1.1.2	96	Wildcard certificates and new gTLDs	2013-02-20	2013-02-20
1.1.3	97	Prevention of Unknown Certificate Contents	2013-02-21	2013-02-21
1.1.4	99	Add DSA Keys (BR v.1.1.4)	2013-05-03	2013-05-03
1.1.5	102	Revision to subject domainComponent language in Section 9.2.3	2013-05-31	2013-05-31
1.1.6	105	Technical Constraints for Subordinate Certificate Authorities	2013-07-29	2013-07-29
1.1.7	112	Replace Definition of “Internal Server Name” with “Internal Name”	2014-04-03	2014-04-03
1.1.8	120	Affiliate Authority to Verify Domain	2014-06-05	2014-06-05
1.1.9	129	Clarification of PSL mentioned in Section 11.1.3	2014-08-04	2014-08-04
1.2.0	125	CAA Records	2014-10-14	2015-04-15
1.2.1	118	SHA-1 Sunset	2014-10-16	2014-11-16
1.2.2	134	Application of RFC 5280 to Pre-certificates	2014-10-16	2014-10-16
1.2.3	135	ETSI Auditor Qualifications	2014-10-16	2014-10-16
1.2.4	144	Validation Rules for .onion Names	2015-02-18	2015-02-18
1.2.5	148	Issuer Field Correction	2015-04-02	2015-04-02
1.3.0	146	Convert Baseline Requirements to RFC 3647 Framework	2015-04-16	2015-04-16
1.3.1	151	Addition of Optional OIDs for Indicating Level of Validation	2015-09-28	2015-09-28
1.3.2	156	Amend Sections 1 and 2 of Baseline Requirements	2015-12-03	2016-12-03
1.3.3	160	Amend Section 4 of Baseline Requirements	2016-02-04	2016-02-04
1.3.4	162	Sunset of Exceptions	2016-03-15	2016-03-15
1.3.5	168	Baseline Requirements Corrections (Revised)	2016-05-10	2016-05-10
1.3.6	171	Updating ETSI Standards in CABF documents	2016-07-01	2016-07-01
1.3.7	164	Certificate Serial Number Entropy	2016-07-08	2016-09-30
1.3.8	169	Revised Validation Requirements	2016-08-05	2017-03-01
1.3.9	174	Reform of Requirements Relating to Conflicts with Local Law	2016-08-29	2016-11-27
1.4.0	173	Removal of requirement to cease use of public key due to incorrect info	2016-07-28	2016-09-11

DRAFT

Ver.	Ballot	Description	Adopted	Effective*
1.4.1	175	Addition of givenName and surname	2016-09-07	2016-09-07
1.4.2	181	Removal of some validation methods listed in Section 3.2.2.4	2017-01-07	2017-01-07
1.4.3	187	Make CAA Checking Mandatory	2017-03-08	2017-09-08
1.4.4	193	825-day Certificate Lifetimes	2017-03-17	2018-03-01
1.4.5	189	Amend Section 6.1.7 of Baseline Requirements	2017-04-14	2017-05-14
1.4.6	195	CAA Fixup	2017-04-17	2017-05-18
1.4.7	196	Define “Audit Period”	2017-04-17	2017-05-18
1.4.8	199	Require commonName in Root and Intermediate Certificates	2017-05-09	2017-06-08
1.4.9	204	Forbid DTPs from doing Domain/IP Ownership	2017-07-11	2017-08-11
1.5.0	212	Canonicalise formal name of the Baseline Requirements	2017-09-01	2017-10-01
1.5.1	197	Effective Date of Ballot 193 Provisions	2017-05-01	2017-06-02
1.5.2	190	Add Validation Methods with Minor Corrections	2017-09-19	2017-10-19
1.5.3	214	CAA Discovery CNAME Errata	2017-09-27	2017-10-27
1.5.4	215	Fix Ballot 190 Errata	2017-10-04	2017-11-05
1.5.5	217	Sunset RFC 2527	2017-12-21	2018-03-09
1.5.6	218	Remove validation methods #1 and #5	2018-02-05	2018-03-09
1.5.7	220	Minor Cleanups (Spring 2018)	2018-03-30	2018-04-29
1.5.8	219	Clarify handling of CAA Record Sets with no “issue”/“issuewild” property tag	2018-04-10	2018-05-10
1.5.9	223	Update BR Section 8.4 for CA audit criteria	2018-05-15	2018-06-14
1.6.0	224	WhoIs and RDAP	2018-05-22	2018-06-22
1.6.1	SC006	Revocation Timeline Extension	2018-09-14	2018-10-14
1.6.2	SC012	Sunset of Underscores in dNSNames	2018-11-09	2018-12-10
1.6.3	SC013	CAA Contact Property and Associated E-mail Validation Methods	2018-12-25	2019-02-01
1.6.4	SC014	Updated Phone Validation Methods	2019-01-31	2019-03-16
1.6.4	SC015	Remove Validation Method Number 9	2019-02-05	2019-03-16
1.6.4	SC007	Update IP Address Validation Methods	2019-02-08	2019-03-16
1.6.5	SC016	Other Subject Attributes	2019-03-15	2019-04-16
1.6.6	SC019	Phone Contact with DNS CAA Phone Contact v2	2019-05-20	2019-09-09

DRAFT

Ver.	Ballot	Description	Adopted	Effective*
1.6.7	SC023	Precertificates	2019-11-14	2019-12-19
1.6.7	SC024	Fall Cleanup v2	2019-11-12	2019-12-19
1.6.8	SC025	Define New HTTP Domain Validation Methods v2	2020-01-31	2020-03-03
1.6.9	SC027	Version 3 Onion Certificates	2020-02-19	2020-03-27
1.7.0	SC029	Pandoc-Friendly Markdown Formatting Changes	2020-03-20	2020-05-04
1.7.1	SC030	Disclosure of Registration / Incorporating Agency	2020-07-13	2020-08-20
1.7.1	SC031	Browser Alignment	2020-07-16	2020-08-20
1.7.2	SC033	TLS Using ALPN Method	2020-08-14	2020-09-22
1.7.3	SC028	Logging and Log Retention	2020-09-10	2020-10-19
1.7.3	SC035	Cleanups and Clarifications	2020-09-09	2020-10-19
1.7.4	SC041	Reformat the BRs, EVGs, and NCSSRs	2021-02-24	2021-04-05
1.7.5	SC042	398-day Re-use Period	2021-04-22	2021-06-02
1.7.6	SC044	Clarify Acceptable Status Codes	2021-04-30	2021-06-03
1.7.7	SC046	Sunset the CAA Exception for DNS Operator	2021-06-02	2021-07-12
1.7.8	SC045	Wildcard Domain Validation	2021-06-02	2021-07-13
1.7.9	SC047	Sunset subject:organizationalUnitName	2021-06-30	2021-08-16
1.8.0	SC048	Domain Name and IP Address Encoding	2021-07-22	2021-08-25
1.8.1	SC050	Remove the requirements of 4.1.1	2021-11-22	2021-12-23
1.8.2	SC053	Sunset for SHA-1 OCSP Signing	2022-01-26	2022-03-04
1.8.3	SC051	Reduce and Clarify Log and Records Archival Retention Requirements	2022-03-01	2022-04-15
1.8.4	SC054	Onion Cleanup	2022-03-24	2022-04-23
1.8.5	SC056	2022 Cleanup	2022-10-25	2022-11-30
1.8.6	SC058	Require distributionPoint in sharded CRLs	2022-11-07	2022-12-11
1.8.7	SC061	New CRL entries must have a Revocation Reason Code	2023-04-01	2023-07-15
2.0.0	SC062	Certificate Profiles Update	2023-04-22	2023-09-15
2.0.1	SC063	Make OCSP optional, require CRLs, and incentivize automation	2023-08-17	2024-03-15
2.0.2	SC066	2023 Cleanup	2023-11-23	2024-01-08
2.0.3	SC069	Clarify router and firewall logging requirements	2024-03-13	2024-04-15
2.0.4	SC065	Convert EVGs into RFC 3647 format	2024-03-15	2024-05-15

DRAFT

Ver.	Ballot	Description	Adopted	Effective*
2.0.5	SC073	Compromised and weak keys	2024-05-03	2024-07-01
2.0.6	SC075	Pre-sign linting	2024-06-28	2024-08-06
2.0.7	SC067	Require Multi-Perspective Issuance Corroboration	2024-08-02	2024-09-06
2.0.8	SC077	Update WebTrust Audit name in Section 8.4 and References	2024-09-02	2024-10-02
2.0.9	SC078	Subject organizationName alignment for DBA / Assumed Name	2024-10-02	2024-11-08
2.1.0	SC076	Clarify and improve OCSP requirements	2024-09-26	2024-11-14
2.1.1	SC079	Allow more than one Certificate Policy in a Cross-Certified Subordinate CA Certificate	2024-09-30	2024-11-14
2.1.2	SC080	Strengthen WHOIS lookups and Sunset Methods 3.2.2.4.2 and 3.2.2.4.15	2024-11-07	2024-12-16
2.1.3	SC083	Winter 2024-2025 Cleanup Ballot	2025-01-23	2025-02-24
2.1.4	SC084	DNS Labeled with ACME Account ID Validation Method	2025-01-28	2025-03-01
2.1.5	SC081	Introduce Schedule of Reducing Validity and Data Reuse Periods	2025-04-11	2025-05-16
2.1.6	SC085	Require Validation of DNSSEC (when present) for CAA and DCV Lookups	2025-06-19	2025-07-21
2.1.7	SC089	Mass Revocation Planning	2025-07-23	2025-08-25
2.1.8	SC092	Sunset Precertificate Signing CAs	2025-10-03	2025-11-04
2.1.9	SC088	DNS TXT Record with Persistent Value DCV Method	2025-10-09	2025-11-10
2.2.0	SC086	Sunset the Inclusion of Address and Routing Parameter Area Names	2025-11-13	2025-12-15
2.2.1	SC091	Sunset 3.2.2.5.3 Reverse Address Lookup Validation,	2025-11-13	2025-12-16
2.2.1	SC091	new DNS-based validation using Persistent DCV TXT Record for IP addresses	2025-11-13	2025-12-16
2.2.2	SC090	Gradually sunset remaining email-based, phone-based, and 'crossover' validation methods	2025-11-20	2026-01-12
2.2.3	SC094	DNSSEC exception in email DCV methods	2026-01-15	2026-02-16
2.2.4	SC096	Carve-out for DNSSEC verification logging requirements	2026-01-14	2026-02-17

DRAFT

Ver.	Ballot	Description	Adopted	Effective*
2.2.5	SC097	Sunset all remaining use of SHA-1 signatures in Certificates and CRLs	2026-02-24	2026-02-25
2.2.6	SC095	Clean-up 2025	2026-02-27	2026-03-31
2.2.7	SC099	Improve Recording of Validation Method	2026-04-18	2026-05-19
2.2.8	SC098	Process RFC 8657 CAA Parameters	2026-05-13	2026-06-16
2.2.9	SC101	Clarify Authorization Domain Names	2026-07-02	2026-08-06
2.3.0	SC100	DNSSEC Clarification and Consolidation	2026-08-06	2026-09-07
2.3.1	SC104	Set presence of AIA extension to SHOULD for Subscriber Certificates	2026-09-03	2026-10-04

* Effective Date and Additionally Relevant Compliance Date(s)

1.2.2 Relevant Dates

Compliance	Section(s)	Summary Description (See Full Text for Details)
2025-01-15	4.9.9	Subscriber Certificate OCSP responses MUST be available 15 minutes after issuance.
2025-01-15	3.2.2.4	CAs MUST NOT rely on HTTPS websites to identify Domain Contact information. CAs MUST rely on IANA resources for identifying Domain Contact information.
2025-03-15	4.3.1.2	The CA SHALL implement a Linting process to test the technical conformity of the to-be-issued Certificate with these Requirements.
2025-03-15	8.7	The CA SHOULD use a Linting process to test the technical accuracy of already issued Certificates against the sample set chosen for Self-Audits.
2025-03-15	3.2.2.9	CAs MUST corroborate the results of domain validation and CAA checks from multiple Network Perspectives where specified.
2025-07-15	3.2.2.4	CAs MUST NOT rely on Methods 3.2.2.4.2 and 3.2.2.4.15 to issue Subscriber Certificates.
2025-12-01	5.7.1.2	CAs SHALL assert in section 5.7.1 of their CPS or combined CP/CPS their mass revocation plan, testing, and continuous improvements.
2026-03-15	3.2.2.4	DNSSEC validation MUST be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective.
2026-03-15	3.2.2.4	CAs MUST NOT use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.

DRAFT

Compliance	Section(s)	Summary Description (See Full Text for Details)
2026-03-15	3.2.2.4	CAs MUST NOT rely on Method 3.2.2.4.8 to issue Subscriber Certificates.
2026-03-15	4.2.2.2.2	DNSSEC validation MUST be performed on all DNS queries associated with CAA record lookups performed by the Primary Network Perspective.
2026-03-15	4.2.2.2.4	CAs MUST NOT use local policy to disable DNSSEC validation on any DNS query associated CAA record lookups.
2026-03-15	4.2.2.2.5	DNSSEC-validation errors observed by the Primary Network Perspective (e.g., SERVFAIL) MUST NOT be treated as permission to issue.
2026-03-15	4.2.1	Subject Identity Information validation maximum data reuse period is 398 days.
2026-03-15	4.2.1	Domain Name and IP Address validation maximum data reuse period is 200 days.
2026-03-15	4.2.2	CAs SHALL NOT issue Certificates containing Domain Names that end in an IP Reverse Zone Suffix.
2026-03-15	6.3.2	Maximum validity period of Subscriber Certificates is 200 days.
2026-03-15	7.1.2.4	CAs MUST NOT use Precertificate Signing CAs to issue Precertificates. CAs MUST NOT issue certificates using the Technically Constrained Precertificate Signing CA Certificate Profile specified in Section 7.1.2.4.
2026-07-15	5.4.1	Audit logs of verification activity MUST include specific information.
2026-09-15	7.1.3.2.1	Sunset all remaining use of SHA-1 in Certificates and CRLs.
2026-11-15	3.2.2.4	Authorization Domain Names must be derived based on the validation method to be used.
2027-03-15	3.2.2.4 and 3.2.2.5	CAs MUST NOT rely on Methods 3.2.2.4.16, 3.2.2.4.17, 3.2.2.5.2, and 3.2.2.5.5 to issue Subscriber Certificates.
2027-03-15	3.2.2.5.3	CAs MUST NOT rely on Method 3.2.2.5.3 to issue Subscriber Certificates.
2027-03-15	4.2.1	Domain Name and IP Address validation maximum data reuse period is 100 days.
2027-03-15	6.3.2	Maximum validity period of Subscriber Certificates is 100 days.
2027-03-15	4.2.2.1.2	CAs MUST process the `accounturi` and `validationmethods` parameters as specified in RFC 8657.

DRAFT

Compliance	Section(s)	Summary Description (See Full Text for Details)
2027-03-15	4.2.2.1.2	If the CA does not identify the Subscriber account via an ACME Account URL as described in RFC 8555, the CA MUST define the supported format of the `accounturi` in Section 4.2 of their CP and/or CPS, and SHOULD comply with the `acct` URI scheme defined in RFC 7565
2028-03-15	3.2.2.4 and 3.2.2.5	CAs MUST NOT rely on Methods 3.2.2.4.4, 3.2.2.4.13, and 3.2.2.4.14 to issue Subscriber Certificates.
2029-03-15	4.2.1	Domain Name and IP Address validation maximum data reuse period is 10 days.
2029-03-15	6.3.2	Maximum validity period of Subscriber Certificates is 47 days.

1.3 PKI Participants

The CA/Browser Forum is a voluntary organization of Certification Authorities and suppliers of Internet browser and other relying-party software applications.

1.3.1 Certification Authorities

Certification Authority (CA) is defined in Section 1.6. Current CA Members of the CA/Browser Forum are listed here: https://cabforum.org/members.

1.3.2 Registration Authorities

With the exception of Section 3.2.2.4, Section 3.2.2.5 and (effective 2026-03-15) Section 3.2.2.8, the CA MAY delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 3.2.

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

1. Meet the qualification requirements of Section 5.3.1, when applicable to the delegated function;
2. Retain documentation in accordance with Section 5.5.2;
3. Abide by the other provisions of these Requirements that are applicable to the delegated function; and
4. Comply with
    a. the CA's Certificate Policy/Certification Practice Statement or
    b. the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.

DRAFT

The CA MAY designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization.

The CA SHALL NOT accept certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. The CA 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, the CA 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, the CA 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 Section 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.

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

1.3.3 Subscribers

As defined in Section 1.6.1.

In some situations, a CA acts as an Applicant or Subscriber, for instance, when it generates and protects a Private Key, requests a Certificate, demonstrates control of a Domain, or obtains a Certificate for its own use.

1.3.4 Relying Parties

"Relying Party" and "Application Software Supplier" are defined in Section 1.6.1. Current Members of the CA/Browser Forum who are Application Software Suppliers are listed here: https://cabforum.org/members.

1.3.5 Other Participants

Other groups that have participated in the development of these Requirements include the AICPA/CICA WebTrust for Certification Authorities task force and ETSI ESI. Participation by such groups does not imply their endorsement, recommendation, or approval of the final product.

DRAFT

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The primary goal of these Requirements is to enable efficient and secure electronic communication, while addressing user concerns about the trustworthiness of Certificates. These Requirements also serve to inform users and help them to make informed decisions when relying on Certificates.

1.4.2 Prohibited Certificate Uses

No stipulation.

1.5 Policy administration

The Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates present criteria established by the CA/Browser Forum for use by Certification Authorities when issuing, maintaining, and revoking publicly-trusted TLS Server Certificates. This document may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Because one of the primary beneficiaries of this document is the end user, the Forum openly invites anyone to make recommendations and suggestions by email to the CA/Browser Forum at questions@cabforum.org. The Forum members value all input, regardless of source, and will seriously consider all such input.

1.5.1 Organization Administering the Document

No stipulation.

1.5.2 Contact Person

Contact information for the CA/Browser Forum is available here: https://cabforum.org/leadership/. In this section of a CA's CPS, the CA shall provide a link to a web page or an email address for contacting the person or persons responsible for operation of the CA.

1.5.3 Person Determining CPS suitability for the policy

No stipulation.

1.5.4 CPS approval procedures

No stipulation.

DRAFT

1.6 Definitions and Acronyms

The Definitions found in the CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein.

1.6.1 Definitions

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 the CA or is the CA.

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 Section 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 these Requirements.

Authorization Domain Name: The FQDN used to perform validation of domain authorization or control for a given FQDN or Wildcard Domain Name.

DRAFT

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

Base Domain Name: The portion of a given 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.

CAA: 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."

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).

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

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 the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

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 Certificate content and Certificate extensions, e.g. a Section in a CA's CPS or a certificate template file used by CA software.

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.

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.

DRAFT

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

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.

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

DNS CAA Email Contact: The email address defined in Appendix A.1.1.

DNS CAA Phone Contact: The phone number defined in Appendix A.1.2.

DNS TXT Record Email Contact: The email address defined in Appendix A.2.1.

DNS TXT Record Phone Contact: The phone number defined in Appendix A.2.2.

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 Namespace: The set of all possible Domain Names that are subordinate to a single 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.

DRAFT

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 assignees).

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

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

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

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.).

~~**High Risk Certificate Request**: A Request that the CA 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 that the CA identifies using its own risk-mitigation criteria.~~

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.

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

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.

DRAFT

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.

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."

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

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 these Requirements.

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.

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."

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

DRAFT

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.

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.

Persistent DCV TXT Record: A DNS TXT record identifying an Applicant in accordance with Section 3.2.2.4.22.

Precertificate: A Precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC 6962 and containing the critical poison extension (OID: 1.3.6.1.4.1.11129.2.4.3).

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).

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.

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.

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.

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.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2.

Random Value: A value specified by a CA 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.

Registration Authority (RA): 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.

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.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

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.

Request Token: A value, derived in a method specified by the CA which binds this demonstration of control to the certificate request. The CA SHOULD define within its CPS (or a document clearly referenced by the CPS) the format and method of Request Tokens it accepts.

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.

DRAFT

A Request Token that does not include a timestamp is valid for a single use and the CA 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.

Note: Examples of Request Tokens include, but are not limited to:

i. a hash of the public key; or
ii. a hash of the Subject Public Key Info [X.509]; or
iii. a hash of a PKCS#10 CSR.

A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests.

Note: This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. `echo \`date -u +%Y%m%d%H%M\` \`sha256sum <r2.csr\` \| sed "s/[ -]//g"` The script outputs:
`201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f`

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

Requirements: The Baseline Requirements found in this document.

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

Reverse Zone Domain Name: the FQDN in the `.arpa` namespace that corresponds to an IP address. This FQDN is constructed by converting the IP address to a sequence of labels followed by the applicable IP Reverse Zone Suffix, as specified in RFC 1035 (for IPv4 addresses) and RFC 3596 (for IPv6 addresses).

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

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.

DRAFT

Short-lived Subscriber Certificate: For Certificates issued on or after 2024-03-15 and prior to 2026-03-15, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 2026-03-15, 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.

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 or an IP Address 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.

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.

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 of this document, 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 the CA or is the CA.

Test Certificate: This term is no longer used in these Baseline Requirements.

Top-Level Domain: From RFC 8499 (https://tools.ietf.org/html/rfc8499): “A Top-Level Domain is a zone that is one layer below the root, such as”com” or “jp”.”

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

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

DRAFT

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

Validation Specialist: Someone who performs the information verification duties specified by these Requirements.

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

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.

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

Acronym	Meaning
AICPA	American Institute of Certified Public Accountants
ADN	Authorization Domain Name
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization

DRAFT

Acronym	Meaning
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VoIP	Voice Over Internet Protocol

1.6.3 References

ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

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.

ISO 21188:2018, Public key infrastructure for financial services – Practices and policy framework.

Network and Certificate System Security Requirements, Version 1.7, available at https://cabforum.org/network-security-requirements/

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-89.pdf.

DRAFT

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

RFC 3492, Request for Comments: 3492, Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA). A. Costello. March 2003.

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

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

RFC 3986, Request for Comments: 3986, Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee, et al. January 2005.

RFC 4035, Request for Comments: 4035, Protocol Modifications for the DNS Security Extensions. R. Arends, et al. March 2005.

RFC 4509, Request for Comments: 4509, Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs). W. Hardaker. May 2006.

RFC 5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments. A. Deacon, et al. September 2007.

RFC 5155, Request for Comments: 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. B. Laurie, et al. March 2008.

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

RFC 5702, Request for Comments: 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC. J. Jansen. October 2009.

RFC 5890, Request for Comments: 5890, Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework. J. Klensin. August 2010.

RFC 5952, Request for Comments: 5952, A Recommendation for IPv6 Address Text Representation. S. Kawamura, et al. August 2010.

RFC 6840, Request for Comments: 6840, Clarifications and Implementation Notes for DNS Security (DNSSEC). S. Weiler, et al. February 2013.

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

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

DRAFT

RFC 7231, Request For Comments: 7231, Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. R. Fielding, et al. June 2014.

RFC 7482, Request for Comments: 7482, Registration Data Access Protocol (RDAP) Query Format. A. Newton, et al. March 2015.

RFC 7538, Request For Comments: 7538, The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect). J. Reschke. April 2015.

RFC 7565, Request for Comments: 7565, The 'acct' URI Scheme. P. Saint-Andre. May 2015.

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

RFC 8555, Request for Comments: 8555, Automatic Certificate Management Environment (ACME). R. Barnes, et al. March 2019.

RFC 8657, Request for Comments: 8657, Certification Authority Authorization (CAA) Record Extensions for Account URI and Automatic Certificate Management Environment (ACME) Method Binding. H. Landau, et al. November 2019.

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

RFC 8738, Request for Comments: 8738, Automated Certificate Management Environment (ACME) IP Identifier Validation Extension. R.B.Shoemaker, Ed. February 2020.

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

RFC 9082, Request for Comments: 9082, Registration Data Access Protocol (RDAP) Query Format. S. Hollenbeck, A. Newton, et al. June 2021.

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

WebTrust Principles and Criteria for Certification Authorities – SSL Baseline.

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

DRAFT

1.6.4 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in these Requirements shall be interpreted in accordance with RFC 2119.

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

DRAFT

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The CA SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with this Policy.

2.2 Publication of information

The CA SHALL publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see Section 8.4).

The CA SHALL develop, implement, enforce, and at least once every 366 days update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements.

The Certificate Policy and/or Certification Practice Statement MUST be structured in accordance with RFC 3647 and MUST include all material required by RFC 3647.

The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version. The CA MAY fulfill this requirement by incorporating these Requirements directly into its Certificate Policy and/or Certification Practice Statements or by incorporating them by reference using a clause such as the following (which MUST include a link to the official version of these Requirements):

[Name of CA] conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates published at https://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are:

i. valid,
ii. revoked, and
iii. expired.

2.3 Time or frequency of publication

The CA SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. The CA SHALL indicate conformance with

this requirement by incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

2.4 Access controls on repositories

The CA shall make its Repository publicly available in a read-only manner.

DRAFT

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

3.1.2 Need for names to be meaningful

3.1.3 Anonymity or pseudonymity of subscribers

3.1.4 Rules for interpreting various name forms

3.1.5 Uniqueness of names

3.1.6 Recognition, authentication, and role of trademarks

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

3.2.2 Authentication of Organization and Domain Identity

If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the `countryName` field, then the CA SHALL verify the country associated with the Subject using a verification process meeting the requirements of Section 3.2.2.3 and that is described in the CA's Certificate Policy and/or Certification Practice Statement. If the Applicant requests a Certificate that will contain the `countryName` field and other Subject Identity Information, then the CA 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 this Section 3.2.2.1 and that is described in the CA's Certificate Policy and/or Certification Practice Statement. The CA SHALL inspect any document relied upon under this Section for alteration or falsification.

3.2.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

DRAFT

2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

Alternatively, the CA 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 the CA determines to be reliable.

3.2.2.2 DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:

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

3.2.2.3 Verification of Country

If the `subject:countryName` field is present, then the CA SHALL verify the country associated with the Subject using one of the following:

a. the IP Address range assignment by country for either
    i. the web site's IP address, as indicated by the DNS record for the web site or
    ii. the Applicant's IP address;
b. the ccTLD of the requested Domain Name;
c. information provided by the Domain Name Registrar; or
d. a method identified in Section 3.2.2.1.

The CA SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

DRAFT

3.2.2.4 Validation of Domain Authorization or Control

Prior to 2026-11-15, the CA SHALL adhere to Section 3.2.2.4 (and its subsections) of these Requirements *or* Section 3.2.2.4 of Version 2.2.7 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates. Effective 2026-11-15, the CA SHALL adhere to Section 3.2.2.4 of these Requirements.

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

The CA MUST follow this process when choosing the Authorization Domain Name (ADN) for validation of each applied-for FQDN or Wildcard Domain Name:

1. Initialize A to the applied-for FQDN or Wildcard Domain Name.
2. Choose a validation method. If A is a Wildcard Domain Name, the CA MUST choose a validation method with a check in the Wildcard column below. If A is an Onion Domain Name, the CA MUST choose a validation method with a check in the Onion column below.
3. If A is an FQDN:
    1. If the validation method has a check in the CNAME column below, the CA MAY replace A with the result of a DNS CNAME lookup of A. This step may be repeated.
    2. If the validation method has a check in the Prune column below and A is not equal to the Base Domain Name of A, the CA MAY replace A with the result of pruning the leftmost Domain Label from A. This step may be repeated.
4. If A is a Wildcard Domain Name:
    1. Remove "*." from the left-most portion of A.
    2. If the validation method has a check in the Prune column below and A is not equal to the Base Domain Name of A, the CA MAY replace A with the result of pruning the leftmost Domain Label from A. This step may be repeated.
5. Use A as the ADN.

Method	Wildcard	Prune	CNAME	Onion
3.2.2.4.4 Constructed Email to Domain Contact	✓	✓	✓	-
3.2.2.4.7 DNS Change	✓	✓	✓	-
3.2.2.4.12 Validating Applicant as a Domain Contact	✓	✓	-	-
3.2.2.4.13 Email to DNS CAA Contact	✓	✓	✓	-
3.2.2.4.14 Email to DNS TXT Contact	✓	✓	✓	-
3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact	✓	✓	✓	-
3.2.2.4.17 Phone Contact with DNS CAA Phone Contact	✓	✓	✓	-
3.2.2.4.18 Agreed-Upon Change to Website v2	-	-	-	✓

DRAFT

Method	Wildcard	Prune	CNAME	Onion
3.2.2.4.19 Agreed-Upon Change to Website - ACME	-	-	-	✓
3.2.2.4.20 TLS Using ALPN	-	-	-	✓
3.2.2.4.21 DNS Labeled with Account ID - ACME	✓	✓	-	-
3.2.2.4.22 DNS TXT Record with Persistent Value	✓	✓	-	-
Appendix B.2.b	✓	✓	-	✓

When the ADN is an Onion Domain Name, the CA SHALL validate it in accordance with Appendix B.

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 the relevant requirement (such as Section 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.

DNSSEC validation MUST be performed in accordance with Section 4.2.2.2 on all DNS queries associated with the validation of domain authorization or control, and CAA record lookups by the Primary Network Perspective.

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, including CNAME lookups performed while choosing the ADN. 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.

For e-mail Domain Validation methods described in sections 3.2.2.4.4, 3.2.2.4.13, 3.2.2.4.14, DNSSEC validation back to the IANA DNSSEC root trust anchor MUST be performed on all DNS CNAME, CAA, TXT queries attempting to obtain the Authorization Domain Name associated with the validation of domain authorization or control by the Primary Network Perspective and CAs MUST NOT use local policy to disable DNSSEC validation. For all other DNS queries, DNSSEC validation back to the IANA DNSSEC root trust anchor SHOULD be performed and CAs SHOULD NOT use local policy to disable DNSSEC validation.

For all other Domain Validation methods, 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 and CAs 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 is considered outside the scope of self-audits performed to fulfill the requirements in Section 8.7.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of the logging requirements of Section 5.4.1.

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. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

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 Email to a Constructed Address

Confirm the Applicant's control over the ADN by:

1. 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 the ADN; and
2. including a Random Value in the email; and
3. receiving a confirming response utilizing the Random Value.

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.

DRAFT

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.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2028: - The CA 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

Confirming the Applicant's control over the ADN by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT or CAA record returned in a query for either:

1. the ADN; or
2. the ADN prefixed with a Domain Label that begins with an underscore character.

If a Random Value is used, the CA 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 Section 4.2.1 of these Guidelines or Section 3.2.2.14.3 of the EV Guidelines).

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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.

If the CA or an Affiliate of the CA operates a DNS zone to which Applicants can delegate (via CNAME) their underscore-prefixed Domain Label, the CA MUST ensure that each Applicant delegates to a unique FQDN within that zone. A CA or Affiliate of a CA

DRAFT

SHOULD NOT operate such a service, and SHOULD direct any Applicants using such a service to use the method described in Section 3.2.2.4.22 instead.

3.2.2.4.8 IP Address

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.

3.2.2.4.9 Test Certificate

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.

3.2.2.4.10 TLS Using a Random Value

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.

3.2.2.4.11 Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant's control over the ADN by validating the Applicant is the Domain Contact for the ADN. This method may only be used if the ADN's Base Domain Name is equal to the ADN. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the ADN.

The Domain Contact for an ADN is: The registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the ADN or as obtained through direct contact with the Domain Name Registrar, or the holder of the email address in an SOA record for the ADN.

When issuing Subscriber Certificates, the CA MUST NOT rely on Domain Contact information obtained using an HTTPS website, regardless of whether previously obtained information is within the allowed reuse period.

When obtaining Domain Contact information for a requested Domain Name the CA: - if using the WHOIS protocol (RFC 3912), MUST query IANA's WHOIS server and follow referrals to the appropriate WHOIS server. - if using the Registry Data Access Protocol (RFC 7482), MUST utilize IANA's bootstrap file to identify and query the correct RDAP server for the domain. - MUST NOT rely on cached 1) WHOIS server information that is

DRAFT

more than 48 hours old, or 2) RDAP bootstrap data from IANA that is more than 48 hours old, to ensure that it relies upon up-to-date and accurate information.

3.2.2.4.13 Email to DNS CAA Contact

Confirming the Applicant's control over the ADN 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 ADNs, provided that each email address is a DNS CAA Email Contact for each ADN being validated. The same email MAY be sent to multiple recipients, provided that each email address is a DNS CAA Email Contact for each ADN 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.

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2028: - The CA 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

Confirming the Applicant's control over the ADN 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 ADN.

Each email MAY confirm control of multiple ADNs, provided that each email address is a DNS TXT Record Email Contact for each ADN being validated. The same email MAY be sent to multiple recipients, provided that each email address is a DNS TXT Record Email Contact for each ADN 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.

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2028: - The CA 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

Confirm the Applicant's control over the ADN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response. Each phone call MAY confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and the recipient of the phone call provides a confirming response for each ADN.

The CA MUST NOT knowingly 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, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA 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. The CPS MAY specify a shorter validity period for Random Values.

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

DRAFT

Effective March 15, 2027: - The CA 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

Confirm the Applicant's control over the ADN 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 the recipient of the phone call provides 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.

The CA 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, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA 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. The CPS MAY specify a shorter validity period for Random Values.

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2027: - The CA 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 ADN 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. the CA 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 ADN, 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 the CA follows redirects, the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer. 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.
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. The CA 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. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

Except for Onion Domain Names, CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over the ADN using the ACME HTTP Challenge method defined in RFC 8555, Section 8.3. The following are additive requirements to RFC 8555.

The CA 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. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

If the CA follows redirects, the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer. 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.

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, CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. token) as the Primary Network Perspective.

3.2.2.4.20 TLS Using ALPN

Confirming the Applicant’s control over the ADN 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. The CPS MAY specify a shorter validity period for the token, in which case the CA MUST follow its CPS.

Except for Onion Domain Names, CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. token) as the Primary Network Perspective.

3.2.2.4.21 DNS Labeled with Account ID - ACME

Confirming the Applicant’s control over the ADN 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. The CPS MAY specify a shorter validity period for the token, in which case the CA MUST follow its CPS.

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same token as the Primary Network Perspective.

3.2.2.4.22 DNS TXT Record with Persistent Value

Confirming the Applicant’s control over the ADN by verifying the presence of a Persistent DCV TXT Record identifying the Applicant. The record MUST be placed at the “`_validation-persist`” label prepended to the ADN being validated (i.e., “`_validation-persist.[Authorization Domain Name]`”).

The CA MUST confirm the Persistent DCV TXT Record's RDATA value fulfills the following requirements:

1. The RDATA value MUST conform to the `issue-value` syntax as defined in RFC 8659, Section 4.2; and
2. The `issuer-domain-name` value MUST be an Issuer Domain Name disclosed by the CA in Section 4.2 of the CA's Certificate Policy and/or Certification Practices Statement; and
3. The `issue-value` MUST contain an `accounturi` parameter, where the parameter value is a unique URI (as described by RFC 8657, Section 3) identifying the account of the Applicant which requested validation for this FQDN; and
4. The `issue-value` MAY contain a `persistUntil` parameter. If present, the parameter value MUST be a base-10 encoded integer representing a UNIX timestamp (the number of seconds since 1970-01-01T00:00:00Z ignoring leap seconds); and
5. The `issue-value` MAY contain additional parameters. CAs MUST ignore any unknown parameter keys.

If the `persistUntil` parameter is present, the CA MUST evaluate its value. If the time of the check is after the time specified in the `persistUntil` parameter value, the CA MUST NOT use the record as evidence of the Applicant's control over the FQDN.

For example, the Persistent DCV TXT Record might look like: `_validation-persist.example.com IN TXT "authority.example; accounturi=https://authority.example/acct/123; persistUntil=1782424856"`

For the purposes of Section 4.2.1, CAs MUST consider 10 days as the maximum validation data reuse period for validations completed using this method.

The following table shows how the `persistUntil` parameter affects whether a DNS record can be used for validation at different points in time:

Examples of how the `persistUntil` parameter affects validation

Date/time of validation	persistUntil	Usable for validation	Explanation
2025-06-15T12:00:00Z	2026-01-01T00:00:00Z (1767225600)	Yes	Validation time is before persistUntil timestamp, so record is usable
2025-06-15T12:00:00Z	2025-01-01T00:00:00Z (1735689600)	No	Validation time is after persistUntil timestamp, so record is not usable

DRAFT

Date/time of validation	persistUntil	Usable for validation	Explanation
2025-06-15T12:00:00Z	(not present)	Yes	No persistUntil parameter present, so no time restriction applies

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe a Persistent DCV TXT Record that demonstrates the Applicant's control over the domain and contains the same `accounturi` parameter as the Primary Network Perspective.

3.2.2.5 Authentication for an IP Address

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of an IP Address listed in a Certificate.

The CA SHALL confirm that prior to issuance, the CA has validated each IP Address listed in the 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 the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

3.2.2.5.1 Agreed-Upon Change to Website

Confirming 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 the CA 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, the CA 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 (such as in Section 4.2.1 of this document).

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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

Confirming 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.

The CA 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.

The CA 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. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2027: - The CA 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

Confirming the Applicant's control over the IP Address by obtaining an FQDN associated with the IP Address through a reverse-IP lookup on the IP Address and then using that FQDN as an ADN and performing validation using a method permitted under Section 3.2.2.4. Effective 2026-11-15, the ADN for this method MUST be exactly the FQDN returned from the reverse-IP lookup; the ADN selection algorithm in section 3.2.2.4 does not apply.

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same FQDN as the Primary Network Perspective.

Effective March 15, 2027: - The CA 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.

3.2.2.5.4 Any Other Method

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.

3.2.2.5.5 Phone Contact with IP Address Contact

Confirming 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. The CA 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, the CA MAY request to be transferred to the IP Address Contact.

In the event of reaching voicemail, the CA may leave the Random Value and the IP Address(es) being validated. The Random Value MUST be returned to the CA 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. The CPS MAY specify a shorter validity period for Random Values.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2027: - The CA 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

Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in RFC 8738.

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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

Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in RFC 8738.

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. token) as the Primary Network Perspective.

3.2.2.5.8 DNS TXT Record with Persistent Value in the Reverse Namespace

Confirming the Applicant's control over the IP Address by converting the IP address to a Reverse Zone Domain Name and then verifying the presence of a Persistent DCV TXT Record identifying the Applicant as defined in Section 3.2.2.4.22. The record MUST be placed at the "`_ip-validation-persist`" label prepended to the Reverse Zone Domain Name of the IP address being validated (i.e., "`_ip-validation-persist.[Reverse Zone Domain Name]`").

3.2.2.6 Wildcard Domain Validation

Before issuing a Wildcard Certificate, the CA MUST establish and follow a documented procedure that determines 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", CAs MUST refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).

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 the Public Suffix List (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. A CA 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.

DRAFT

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA SHOULD consider the following during its evaluation:

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

Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.

3.2.2.8 CAA Records

Refer to Section 4.2.2.1 for CAA record processing requirements.

3.2.2.8.1 DNSSEC Validation of CAA Records

Refer to Section 4.2.2.2 for DNSSEC validation of CAA record processing requirements.

3.2.2.9 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.

The CA 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 the CA 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, 4) Contact Address, or 5) Persistent DCV TXT Record, as required by the relied upon validation method specified in Section 3.2.2.4 and Section 3.2.2.5; and
b. the CA's authority to issue to the requested domain(s), as specified in Section 4.2.2.1.

Section 3.2.2.4 and Section 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.

CAs 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, CAs 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 the CA 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.

A CA 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), ISAE 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.

DRAFT

- 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 Section 8 of these Requirements.

If any of the above considerations are performed by a Delegated Third Party, the CA 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 Section 1.3.2, Delegated Third Parties are not required to be within the audit scope described in Section 8 of these Requirements to satisfy the above considerations.

Phased Implementation Timeline:

- Effective 2025-03-15, the CA MUST implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. The CA 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 2025-09-15, the CA MUST implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. The CA MUST ensure that the requirements defined in Quorum Requirements Table are satisfied. If the requirements are not satisfied, then the CA MUST NOT proceed with issuance of the Certificate.
- Effective 2026-03-15, the CA MUST implement Multi-Perspective Issuance Corroboration using at least three (3) remote Network Perspectives. The CA 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 the CA MUST NOT proceed with issuance of the Certificate.

- Effective 2026-06-15, the CA MUST implement Multi-Perspective Issuance Corroboration using at least four (4) remote Network Perspectives. The CA 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 the CA MUST NOT proceed with issuance of the Certificate.
- Effective 2026-12-15, the CA MUST implement Multi-Perspective Issuance Corroboration using at least five (5) remote Network Perspectives. The CA 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 the CA MUST NOT proceed with issuance of the Certificate.

3.2.3 Authentication of individual identity

If an Applicant subject to this Section 3.2.3 is a natural person, then the CA SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

The CA 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). The CA SHALL inspect the copy for any indication of alteration or falsification.

The CA SHALL verify 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. The CA MAY rely on the same government-issued ID that was used to verify the Applicant's name.

The CA SHALL verify the certificate request with the Applicant using a Reliable Method of Communication.

3.2.4 Non-verified subscriber information

3.2.5 Validation of authority

If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

The CA MAY use the sources listed in Section 3.2.2.1 to verify the Reliable Method of Communication. Provided that the CA uses a Reliable Method of Communication, the CA 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 the CA deems appropriate.

In addition, the CA 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 the CA SHALL NOT accept any certificate requests that are outside this specification. The CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for Interoperation or Certification

The CA SHALL disclose all Cross-Certified Subordinate CA Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross-Certified Subordinate CA Certificate at issue).

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

3.3.2 Identification and authentication for re-key after revocation

3.4 Identification and authentication for revocation request

DRAFT

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

No stipulation.

4.1.2 Enrollment process and responsibilities

Prior to the issuance of a Certificate, the CA SHALL obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement or Terms of Use, which may be electronic.

The CA SHOULD obtain any additional documentation the CA determines necessary to meet these Requirements.

Prior to the issuance of a Certificate, the CA SHALL obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with these Requirements. One certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 4.2.1, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request MAY be made, submitted and/or signed electronically.

The certificate request MUST contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

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 necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA 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. The CA SHALL establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

DRAFT

Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's `subjectAltName` extension.

Section 6.3.2 limits the validity period of Subscriber Certificates.

The CA MAY use the documents and data provided in Section 3.2 to verify certificate information, or may reuse previous validations themselves, including validation of authority, provided that the CA obtained the data or document from a source specified under Section 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
	2026-03-15	825 days
2026-03-15		398 days

For validation of Domain Names and IP Addresses according to Section 3.2.2.4 and Section 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
	2026-03-15	398 days
2026-03-15	2027-03-15	200 days
2027-03-15	2029-03-15	100 days
2029-03-15		10 days

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.

After the change to any validation method specified in the Baseline Requirements or EV Guidelines, a CA may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in Section 4.2.1 unless otherwise specifically provided in a ballot.

~~The CA 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 these Requirements.~~

DRAFT

~~If a Delegated Third Party fulfills any of the CA's obligations under this section, the CA 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 the CA's own processes.~~

4.2.2 Approval or rejection of certificate applications

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

4.2.2.1 CAA record processing

As part of the Certificate issuance process, the CA 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 MUST be described in Section 4.2 of the CA's Certificate Policy and/or Certification Practice Statement, including specifying the set of Issuer Domain Names that the CA recognizes in CAA "issue" or "issuewild" records as permitting it to issue.

CAs MAY check CAA records at any other time.

When processing CAA records, CAs MUST process the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are 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 this document. CAs MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set.

If the CA issues a 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 CAs "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 these Baseline Requirements, CAs MUST NOT rely on any exceptions specified in their CP or CPS unless they are one of the following:

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

CAs are permitted to treat a record lookup failure as permission to issue if:

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

CAs 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. CAs are not expected to support URL schemes in the iodef record other than mailto: or https:.

DNSSEC validation MUST be performed in accordance with Section 4.2.2.2 on all DNS queries associated with CAA record lookups performed by the Primary Network Perspective.

4.2.2.1.1 CAA Multi-Perspective Issuance Corroboration

Some methods relied upon for validating the Applicant's ownership or control of the subject domain(s) (see Section 3.2.2.4) or IP address(es) (see Section 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 Section 3.2.2.9). 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, a CA 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 Section 4.2.2.1.

4.2.2.1.2 CAA Parameters

When processing CAA records, CAs SHOULD process the `accounturi` and `validationmethods` parameters as specified in RFC 8657. *Effective 2027-03-15*, when processing CAA records, CAs MUST process the `accounturi` and `validationmethods` parameters as specified in RFC 8657.

In addition, *Effective 2027-03-15*: - If the CA does not identify the Subscriber account via an ACME Account URL as described in RFC 8555, the CA MUST define the supported format of the `accounturi` in Section 4.2 of their CP and/or CPS, and SHOULD comply with the 'acct' URI scheme defined in RFC 7565. - For certificate requests made using the ACME protocol, the CA MAY permit the 'accounturi' parameter to identify a primary organizational account (the "Parent Account"). As an explicit exception to Section 3 of RFC 8657, the CA MAY issue a certificate requested by a different account (the "Subordinate ACME Account") if and only if the CA ensures all of the following: 1. The CA maintains an internal, auditable mapping that binds the Subordinate ACME

Account to the Parent Account identified by the 'accounturi'. 2. The CA has cryptographically or administratively verified that the Parent Account explicitly authorized the Subordinate ACME Account to obtain certificates under this mapping. 3. The CA retains audit logs demonstrating this authorization and mapping for the standard data retention period required by these Requirements. - If the CA supports domain validation methods that are not registered in the IANA ACME Validation Methods registry, the CA MUST interpret and process `validationmethods` labels formed by concatenating the string 'ca-tbr-' with the BR 3.2.2.4 subsection number, e.g. 'ca-tbr-7' represents the DNS method described in TLS BR 3.2.2.4.7. If a CA performs domain validation using a mechanism that can be represented by multiple labels (e.g. 'http-01' and 'ca-tbr-19'), the CA SHOULD accept any of the labels as granting permission to issue. - The canonical representation of validationmethods labels is lowercase letters. However, the CA MAY perform case insensitive matching of labels. If the CA does perform case insensitive matching of labels, this practice MUST be documented in their CP and/or CPS.

4.2.2.2 DNSSEC Validation Requirements

This section consolidates all DNSSEC validation requirements applicable to DNS queries performed during domain validation (Section 3.2.2.4) and CAA record processing (Section 4.2.2.1).

4.2.2.2.1 DNS Resolver Requirements

The DNS resolver used by the Primary Network Perspective for all DNS queries associated with the validation of domain authorization or control and for CAA record lookups 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.

4.2.2.2.2 Applicability and Scope

DNSSEC validation MUST be performed by the Primary Network Perspective on all DNS queries associated with:

1. the validation of domain authorization or control as described in Section 3.2.2.4; and
2. CAA record lookups as described in Section 4.2.2.1.

4.2.2.2.3 Email Domain Validation Methods - Partial Exception

For the e-mail-based Domain Validation methods described in sections 3.2.2.4.4, 3.2.2.4.13, and 3.2.2.4.14:

DRAFT

- DNSSEC validation MUST be performed on all DNS CNAME, CAA, and TXT queries performed by the Primary Network Perspective used to obtain the Authorization Domain Name, and CAs MUST NOT use local policy to disable DNSSEC validation on those queries.
- For all other DNS queries associated with these methods performed by the Primary Network Perspective, DNSSEC validation SHOULD be performed and CAs SHOULD NOT use local policy to disable DNSSEC validation.

4.2.2.2.4 Prohibition on Disabling DNSSEC Validation

For all Domain Validation methods other than those listed in Section 4.2.2.2.3, and for all CAA record lookups, CAs MUST NOT use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control or with CAA record lookups performed by the Primary Network Perspective.

4.2.2.2.5 DNSSEC Validation Errors

Except as may be allowed for in section 4.2.2.2.3, DNSSEC-validation errors observed by the Primary Network Perspective (e.g., SERVFAIL) MUST NOT be treated as permission to issue.

4.2.2.2.6 Remote Network Perspectives

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 and for CAA record lookups performed by Remote Network Perspectives as part of Multi-Perspective Issuance Corroboration.

4.2.2.2.7 Exclusions

The full set of DNS lookup information related to DNSSEC validation is considered outside the scope of:

1. self-audits performed to fulfill the requirements in Section 8.7; and
2. the logging requirements of Section 5.4.1.

The above exclusions notwithstanding, the CA MUST retain information sufficient to verify that DNSSEC validation is being carried out in accordance with the requirements contained in the rest of Section 4.2.2.2.

4.2.3 Time to process certificate applications

No stipulation.

DRAFT

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

4.3.1.1 Manual authorization of certificate issuance for Root CAs

Certificate issuance by the Root CA SHALL require an individual authorized by the CA (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 these Requirements, it is considered best practice for the CA to 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 the CA 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, the CA 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.

CAs MAY implement their own certificate Linting tools, but CAs SHOULD use the Linting tools that have been widely adopted by the industry (see https://cabforum.org/resources/tools/).

CAs are encouraged to contribute to open-source Linting projects, such as by:

- creating new or improving existing lints,
- reporting potentially inaccurate linting results as bugs,
- notifying maintainers of Linting software of checks that are not covered by existing lints,
- updating documentation of existing lints, and
- generating test certificates for positive/negative tests of specific lints.

4.3.1.3 Linting of issued Certificates

CAs MAY use a Linting process to test each issued Certificate.

DRAFT

4.3.2 Notification to subscriber by the CA of issuance of certificate

No stipulation.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

No stipulation.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

See Section 9.6.3, provisions 2. and 4.

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

DRAFT

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

No stipulation.

DRAFT

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

The CA MAY support revocation of Short-lived Subscriber Certificates.

With the exception of Short-lived Subscriber Certificates, the CA SHALL revoke a 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, without specifying a CRLreason, that the CA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate, including but not limited to those identified in Section 6.1.1.3(5) (CRLReason #1, keyCompromise);
5. The CA obtains 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,

including cases where the CA failed to perform CAA checking correctly or where issuance was not permitted according to Section 3.2.2.8 (CAA Records) (CRLReason #4, superseded).

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

6. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 (CRLReason #4, superseded);
7. The CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
8. The CA 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);
9. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP 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) (CRLReason #5, cessationOfOperation);
10. ~~The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);~~
10. Removed;
11. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
12. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement (CRLReason #4, superseded);
13. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
14. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
15. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement for a reason that is not otherwise required to be specified by this section 4.9.1.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or
16. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA 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 the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA 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 Section 6.1.5 and Section 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.

4.9.2 Who can request revocation

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for revocation request

The CA SHALL provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in the CA's Certificate Policy or Certification Practice Statement. The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

The CA SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA SHALL publicly disclose the instructions through a readily accessible online means and in Section 1.5.2 of their CPS.

4.9.4 Revocation request grace period

No stipulation.

DRAFT

4.9.5 Time within which CA must process the revocation request

Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the CA 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 which the CA 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 Section 4.9.1.1. The date selected by the CA SHOULD consider 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 Reports 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 they didn't receive the goods they ordered); and
5. Relevant legislation.

4.9.6 Revocation checking requirement for relying parties

No stipulation.

Note: Following certificate issuance, a certificate may be revoked for reasons stated in Section 4.9. Therefore, relying parties should check the revocation status of all certificates that contain a CDP or OCSP pointer.

4.9.7 CRL issuance frequency

CRLs MUST be available via a publicly-accessible HTTP URL (i.e., "published").

Within twenty-four (24) hours of issuing its first Certificate, the CA MUST 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.

CAs issuing Subscriber Certificates:

DRAFT

1. MUST update and publish a new CRL 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;
2. MUST update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

CAs issuing CA Certificates:

1. MUST update and publish a new CRL at least every twelve (12) months;
2. MUST update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

CAs MUST 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.

4.9.8 Maximum latency for CRLs (if applicable)

No stipulation.

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, 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 the CA 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:

- Effective 2025-01-15, 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, the CA 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, the CA 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, the CA 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 RFC 6960 and/or RFC 5019. 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.

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, 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

No Stipulation.

4.9.12 Special requirements re key compromise

See Section 4.9.1.

DRAFT

4.9.13 Circumstances for suspension

The Repository MUST NOT include entries that indicate that a Certificate is suspended.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.

4.10.2 Service availability

The CA SHALL operate and maintain its CRL and optional OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The CA 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 a Certificate that is the subject of such a complaint.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

DRAFT

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

DRAFT

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

The CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein.

The CA SHALL develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process MUST include:

1. physical security and environmental controls;
2. system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, separate trusted-role assignments, education, awareness, and training; and
5. logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The CA's security program MUST include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST include administrative, organizational, technical, and physical safeguards appropriate to the

DRAFT

sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST also take into account then-available technology and the cost of implementing the specific measures, and SHALL implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical Security Controls

5.1.1 Site location and construction

5.1.2 Physical access

5.1.3 Power and air conditioning

5.1.4 Water exposures

5.1.5 Fire prevention and protection

5.1.6 Media storage

5.1.7 Waste disposal

5.1.8 Off-site backup

5.2 Procedural controls

5.2.1 Trusted roles

5.2.2 Number of Individuals Required per Task

The CA Private Key SHALL be backed up, stored, and recovered only by personnel in Trusted Roles using, at least, dual control in a physically secured environment.

5.2.3 Identification and authentication for each role

5.2.4 Roles requiring separation of duties

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, the CA SHALL verify the identity and trustworthiness of such person.

DRAFT

5.3.2 Background check procedures

5.3.3 Training Requirements and Procedures

The CA SHALL provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.

The CA SHALL maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

The CA SHALL document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

The CA SHALL require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in these Requirements.

5.3.4 Retraining frequency and requirements

All personnel in Trusted roles SHALL maintain skill levels consistent with the CA's training and performance programs.

5.3.5 Job rotation frequency and sequence

5.3.6 Sanctions for unauthorized actions

5.3.7 Independent Contractor Controls

The CA SHALL verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

5.3.8 Documentation supplied to personnel

5.4 Audit logging procedures

5.4.1 Types of events recorded

The CA and each Delegated Third Party SHALL record events related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems. The CA and each Delegated Third Party SHALL record events related to their actions taken to process a certificate request and to issue a

DRAFT

Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. The CA SHALL make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

The CA SHALL record at least the following events:

1. CA certificate and key lifecycle events, including:
    1. Key generation, backup, storage, recovery, archival, and destruction;
    2. Certificate requests, renewal, and re-key requests, and revocation;
    3. Approval and rejection of certificate requests;
    4. Cryptographic device lifecycle management events;
    5. Generation of Certificate Revocation Lists;
    6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10); and
    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    1. Certificate requests, renewal, and re-key requests, and revocation;
    2. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement. Effective 2026-07-15, records MUST include at a minimum:
        1. the information being validated (e.g., the applied-for FQDN or the organization name);
        2. the ADN used (if applicable and different from the applied-for FQDN); and
        3. the validation method used (e.g., the BRs section number or the registered label of an ACME validation method);
    3. Approval and rejection of certificate requests;
    4. Issuance of Certificates;
    5. Generation of Certificate Revocation Lists; and
    6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).
    7. Multi-Perspective Issuance Corroboration attempts from each Network Perspective, minimally recording the following information:
        1. an identifier that uniquely identifies the Network Perspective used;
        2. the attempted domain name and/or IP address; and
        3. the result of the attempt (e.g., "domain validation pass/fail", "CAA permission/prohibition").
    8. 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:

DRAFT

1. Successful and unsuccessful PKI system access attempts;
~~2.~~1. PKI and security system actions performed;
~~3.~~2. Security profile changes;
~~4.~~3. Installation, update and removal of software on a Certificate System;
~~5.~~4. System crashes, hardware failures, and other anomalies;
~~6.~~5. Relevant router and firewall activities (as described in Section 5.4.1.1); and
~~7.~~6. Entries to and exits from the CA facility.

Log records MUST include at least the following elements:

1. Date and time of event;
2. Identity of the person making the journal record (when applicable); and
3. Description of the event.

5.4.1.1 Router and firewall activities logs

Logging of router and firewall activities necessary to meet the requirements of Section 5.4.1, Subsection 3.6 MUST 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

5.4.3 Retention period for audit log

The CA 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 Section 5.4.1 (1)) after the later occurrence of:
    1. the destruction of the CA Private Key; or
    2. 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 Section 5.4.1 (2)) after the expiration of the Subscriber Certificate;
3. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

Note: While these Requirements set the minimum retention period, the CA MAY choose a greater value as more appropriate in order to be able to investigate possible

DRAFT

security or other types of incidents that will require retrospection and examination of past audit log events.

5.4.4 Protection of audit log

5.4.5 Audit log backup procedures

5.4.6 Audit collection System (internal vs. external)

5.4.7 Notification to event-causing subject

5.4.8 Vulnerability assessments

Additionally, the CA's security program MUST include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.5 Records archival

5.5.1 Types of records archived

The CA and each Delegated Third Party SHALL archive all audit logs (as set forth in Section 5.4.1).

Additionally, the CA 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.

5.5.2 Retention period for archive

Archived audit logs (as set forth in Section 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 Section 5.4.3, whichever is longer.

Additionally, the CA and each Delegated Third Party SHALL retain, for at least two (2) years:

DRAFT

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 Section 5.5.1); and
2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of:
    1. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
    2. the expiration of the Subscriber Certificates relying upon such records and documentation.

Note: While these Requirements set the minimum retention period, the CA 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.

5.5.3 Protection of archive

5.5.4 Archive backup procedures

5.5.5 Requirements for time-stamping of records

5.5.6 Archive collection system (internal or external)

5.5.7 Procedures to obtain and verify archive information

5.6 Key changeover

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

5.7.1.1 Incident Response and Disaster Recovery Plans

CA organizations shall have an Incident Response Plan and a Disaster Recovery Plan.

The CA SHALL document a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The CA is not required to publicly disclose its business continuity plans but SHALL make its business continuity plan and security plans available to the CA's auditors upon request. The CA SHALL annually test, review, and update these procedures.

The business continuity plan MUST include:

1. The conditions for activating the plan,

2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

5.7.1.2 Mass Revocation Plans

CA organizations MUST have a mass revocation plan, and as of 2025-12-01, they SHALL assert in section 5.7.1 of their CPS or combined CP/CPS that they maintain a comprehensive and actionable plan for mass revocation events, that they perform annual testing of the mass revocation plan, and that they incorporate lessons learned into such plan in order to continually improve their preparedness for mass revocation events over time.

The CA's mass revocation plan MUST include clearly defined, actionable, and comprehensive procedures designed to ensure rapid, consistent, and reliable response to large-scale certificate revocation scenarios. The CA is not required to publicly disclose its mass revocation plan or procedures but MUST make them available to its auditors upon request. The CA SHALL annually test, review, and update its plan and such procedures. The CA's mass revocation plan MAY be integrated into the CA'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 MUST 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;

DRAFT

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

5.7.3 Recovery Procedures after Key Compromise

5.7.4 Business continuity capabilities after a disaster

5.8 CA or RA termination

DRAFT

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA Key Pair Generation

For CA Key Pairs that are either:

i. used as a CA Key Pair for a Root Certificate or
ii. used as a CA Key Pair for a Subordinate CA Certificate, where the Subordinate CA is not the operator of the Root CA or an Affiliate of the Root CA,

the CA SHALL:

1. prepare and follow a Key Generation Script,
2. have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process, and
3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs that are for the operator of the Root CA or an Affiliate of the Root CA, the CA SHOULD:

1. prepare and follow a Key Generation Script and
2. have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process.

In all cases, the CA SHALL:

1. generate the CA Key Pair in a physically secured environment as described in the CA's Certificate Policy and/or Certification Practice Statement;
2. generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;
3. generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement;
4. log its CA Key Pair generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

DRAFT

6.1.1.2 RA Key Pair Generation

6.1.1.3 Subscriber Key Pair Generation

The CA 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 Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. The CA has previously been notified that the Applicant's Private Key has suffered a Key Compromise using the CA's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12;
5. The Public Key corresponds to an industry-demonstrated weak Private Key. At least the following precautions SHALL be implemented:
    1. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), the CA 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 Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, the CA SHALL reject Debian weak keys.
    2. In the case of ROCA vulnerability, the CA SHALL reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
    3. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), the CA SHALL reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

    Suggested tools for checking for weak keys can be found here: https://cabforum.org/resources/tools/

If the Subscriber Certificate will contain an `extKeyUsage` extension containing either the values `id-kp-serverAuth` RF 5280 or `anyExtendedKeyUsage` RF 5280, the CA 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 the CA.

6.1.2 Private key delivery to subscriber

Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key without authorization by the Subscriber.

If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

DRAFT

6.1.3 Public key delivery to certificate issuer

6.1.4 CA public key delivery to relying parties

6.1.5 Key sizes

For RSA key pairs the CA SHALL:

- Ensure that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs, the CA SHALL:

- Ensure that the key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve.

No other algorithms or key sizes are permitted.

6.1.6 Public key parameters generation and quality checking

RSA: The CA 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: The CA SHOULD 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]

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Private Keys corresponding to Root Certificates MUST NOT be used to sign Certificates except in the following cases:

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 (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified in Section 6.2.7 MUST consist of physical security, encryption, or a

combination of both, implemented in a manner that prevents disclosure of the Private Key. The CA 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

6.2.2 Private key (n out of m) multi-person control

6.2.3 Private key escrow

6.2.4 Private key backup

See Section 5.2.2.

6.2.5 Private key archival

Parties other than the Subordinate CA SHALL NOT archive the Subordinate CA Private Keys without authorization by the Subordinate CA.

6.2.6 Private key transfer into or from a cryptographic module

If the Issuing CA generated the Private Key on behalf of the Subordinate CA, then the Issuing CA SHALL encrypt the Private Key for transport to the Subordinate CA. If the Issuing CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the Issuing CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private key storage on cryptographic module

The CA SHALL protect its Private Key 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.

DRAFT

6.2.8 Activating Private Keys

6.2.9 Deactivating Private Keys

6.2.10 Destroying Private Keys

6.2.11 Cryptographic Module Rating

6.3 Other aspects of key pair management

6.3.1 Public key archival

6.3.2 Certificate operational periods and key pair usage periods

Subscriber Certificates issued before 2026-03-15 SHOULD NOT have a Validity Period greater than 397 days and MUST NOT have a Validity Period greater than 398 days.

Subscriber Certificates issued on or after 2026-03-15 and before 2027-03-15 SHOULD NOT have a Validity Period greater than 199 days and MUST NOT have a Validity Period greater than 200 days.

Subscriber Certificates issued on or after 2027-03-15 and before 2029-03-15 SHOULD NOT have a Validity Period greater than 99 days and MUST NOT have a Validity Period greater than 100 days.

Subscriber Certificates issued on or after 2029-03-15 SHOULD NOT have a Validity Period greater than 46 days and MUST NOT have a Validity Period greater than 47 days.

Reference for maximum Validity Periods of Subscriber Certificates

Certificate issued on or after	Certificate issued before	Maximum Validity Period
	2026-03-15	398 days
2026-03-15	2027-03-15	200 days
2027-03-15	2029-03-15	100 days
2029-03-15		47 days

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, shall represent an additional day. For this reason, Subscriber Certificates SHOULD NOT be issued for the maximum permissible time by default, in order to account for such adjustments.

DRAFT

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.2 Activation data protection

6.4.3 Other aspects of activation data

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer security rating

6.6 Life cycle technical controls

6.6.1 System development controls

If a CA uses Linting software developed by third parties, it SHOULD monitor for updated versions of that software and plan for updates no later than three (3) months from the release of the update.

The CA 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

6.6.3 Life cycle security controls

6.7 Network security controls

6.8 Time-stamping

DRAFT

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The CA SHALL meet the technical requirements set forth in Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking.

The CA SHALL issue Certificates in accordance with the profile specified in these Requirements.

7.1.1 Version number(s)

Certificates MUST be of type X.509 v3.

7.1.2 Certificate Content and Extensions

If the CA asserts compliance with these Baseline Requirements, all certificates that it issues MUST comply with one of the following Certificate Profiles, which incorporate, and are derived from RFC 5280. Except as explicitly noted, all normative requirements imposed by RFC 5280 shall apply, in addition to the normative requirements imposed by this document. CAs SHOULD examine RFC 5280, Appendix B for further issues to be aware of.

- CA Certificates
    - Section 7.1.2.1 - Root CA Certificate Profile
    - Subordinate CA Certificates
        - Cross Certificates
            - Section 7.1.2.2 - Cross-Certified Subordinate CA Certificate Profile
        - Technically Constrained CA Certificates
            - Section 7.1.2.3 - Technically-Constrained Non-TLS Subordinate CA Certificate Profile
            - Section 7.1.2.4 - Technically-Constrained Precertificate Signing CA Certificate Profile
            - Section 7.1.2.5 - Technically-Constrained TLS Subordinate CA Certificate Profile
        - Section 7.1.2.6 - TLS Subordinate CA Certificate Profile
- Section 7.1.2.7 - Subscriber (End-Entity) Certificate Profile
- Section 7.1.2.8 - OCSP Responder Certificate Profile
- Section 7.1.2.9 - Precertificate Profile

7.1.2.1 Root CA Certificate Profile

Field	Description
`tbsCertificate`	
`version`	MUST be v3(2)

Field	Description
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	Encoded value MUST be byte-for-byte identical to the encoded subject
validity	See Section 7.1.2.1.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.1.2
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature
signature	

7.1.2.1.1 Root CA Validity

Field	Minimum	Maximum
notBefore	One day prior to the time of signing	The time of signing
notAfter	2922 days (approx. 8 years)	9132 days (approx. 25 years)

Note: This restriction applies even in the event of generating a new Root CA Certificate for an existing subject and subjectPublicKeyInfo (e.g. reissuance). The new CA Certificate MUST conform to these rules.

7.1.2.1.2 Root CA Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	RECOMMENDED	N	See Section 7.1.2.1.3
basicConstraints	MUST	Y	See Section 7.1.2.1.4
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
extKeyUsage	MUST NOT	-	-
certificatePolicies	NOT RECOMMENDED	N	See Section 7.1.2.10.5
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3

DRAFT

Extension	Presence	Critical	Description
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.1.3 Root CA Authority Key Identifier

Field	Description
`keyIdentifier`	MUST be present. MUST be identical to the `subjectKeyIdentifier` field.
`authorityCertIssuer`	MUST NOT be present
`authorityCertSerialNumber`	MUST NOT be present

7.1.2.1.4 Root CA Basic Constraints

Field	Description
`cA`	MUST be set TRUE
`pathLenConstraint`	NOT RECOMMENDED

7.1.2.2 Cross-Certified Subordinate CA Certificate Profile

This Certificate Profile MAY be used when issuing a CA Certificate using the same Subject Name and Subject Public Key Information as one or more existing CA Certificate(s), whether a Root CA Certificate or Subordinate CA Certificate.

Before issuing a Cross-Certified Subordinate CA, the Issuing CA MUST confirm that the existing CA Certificate(s) are subject to these Baseline Requirements and were issued in compliance with the then-current version of the Baseline Requirements at time of issuance.

Field	Description
`tbsCertificate`	
`version`	MUST be v3(2)
`serialNumber`	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
`signature`	See Section 7.1.3.2
`issuer`	MUST be byte-for-byte identical to the `subject` field of the Issuing CA. See Section 7.1.4.1
`validity`	See Section 7.1.2.2.1
`subject`	See Section 7.1.2.2.2
`subjectPublicKeyInfo`	See Section 7.1.3.1

DRAFT

Field	Description
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.2.3
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.2.1 Cross-Certified Subordinate CA Validity

Field	Minimum	Maximum
notBefore	The earlier of one day prior to the time of signing or the earliest notBefore date of the existing CA Certificate(s)	The time of signing
notAfter	The time of signing	Unspecified

7.1.2.2.2 Cross-Certified Subordinate CA Naming

The subject MUST comply with the requirements of Section 7.1.4, or, if the existing CA Certificate was issued in compliance with the then-current version of the Baseline Requirements, the encoded subject name MUST be byte-for-byte identical to the encoded subject name of the existing CA Certificate.

Note: The above exception allows the CAs to issue Cross-Certified Subordinate CA Certificates, provided that the existing CA Certificate complied with the Baseline Requirements in force at time of issuance. This allows the requirements of Section 7.1.4 to be improved over time, while still permitting Cross-Certification. If the existing CA Certificate did not comply, issuing a Cross-Certificate is not permitted.

7.1.2.2.3 Cross-Certified Subordinate CA Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
basicConstraints	MUST	Y	See Section 7.1.2.10.4
certificatePolicies	MUST	N	See Section 7.1.2.2.6
crlDistributionPoints	MUST	N	See Section 7.1.2.11.2
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
authorityInformationAccess	SHOULD	N	See Section 7.1.2.10.3

DRAFT

Extension	Presence	Critical	Description
nameConstraints	MAY	*[1]	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

In addition to the above, extKeyUsage extension requirements vary based on the relationship between the Issuer and Subject organizations represented in the Cross-Certificate.

The extKeyUsage extension MAY be "unrestricted" as described in the following table if:

- the organizationName represented in the Issuer and Subject names of the corresponding certificate are either:
  - the same, or
  - the organizationName represented in the Subject name is an affiliate of the organizationName represented in the Issuer name
- the corresponding CA represented by the Subject of the Cross-Certificate is operated by the same organization as the Issuing CA or an Affiliate of the Issuing CA organization.

Cross-Certified Subordinate CA with Unrestricted EKU

Extension	Presence	Critical	Description
extKeyUsage	SHOULD[2]	N	See Section 7.1.2.2.4

In all other cases, the extKeyUsage extension MUST be "restricted" as described in the following table:

Cross-Certified Subordinate CA with Restricted EKU

Extension	Presence	Critical	Description
extKeyUsage	MUST[3]	N	See Section 7.1.2.2.5

[1] See Section 7.1.2.10.8 for further requirements, including regarding criticality of this extension.

[2] While RFC 5280, Section 4.2.1.12 notes that this extension will generally only appear within end-entity certificates, these Requirements make use of this extension to further protect relying parties by limiting the scope of CA Certificates, as implemented by a number of Application Software Suppliers.

[3] While RFC 5280, Section 4.2.1.12 notes that this extension will generally only appear within end-entity certificates, these Requirements make use of this extension to further protect relying parties by limiting the scope of CA Certificates, as implemented by a number of Application Software Suppliers.

DRAFT

7.1.2.2.4 Cross-Certified Subordinate CA Extended Key Usage - Unrestricted

Unrestricted Extended Key Usage Purposes (Affiliated Cross-Certified CA)

Key Purpose	Description
`anyExtendedKeyUsage`	The special extended key usage to indicate there are no restrictions applied. If present, this MUST be the only key usage present.
Any other value	CAs MUST NOT include any other key usage with the `anyExtendedKeyUsage` key usage present.

Alternatively, if the Issuing CA does not use this form, then the Extended Key Usage extension, if present, MUST be encoded as specified in Section 7.1.2.2.5.

7.1.2.2.5 Cross-Certified Subordinate CA Extended Key Usage - Restricted

Restricted TLS Cross-Certified Subordinate CA Extended Key Usage Purposes (i.e., for restricted Cross-Certified Subordinate CAs issuing TLS certificates directly or transitively).

TLS Cross-Certified Subordinate CA EKU

Key Purpose	Description
`id-kp-serverAuth`	MUST be present.
`id-kp-clientAuth`	MAY be present.
`id-kp-emailProtection`	MUST NOT be present.
`id-kp-codeSigning`	MUST NOT be present.
`id-kp-timeStamping`	MUST NOT be present.
`anyExtendedKeyUsage`	MUST NOT be present.
Any other value	NOT RECOMMENDED.

Restricted Non-TLS Cross-Certified Subordinate CA Extended Key Usage Purposes (i.e., for restricted Cross-Certified Subordinate CAs not issuing TLS certificates directly or transitively).

Non-TLS Cross-Certified Subordinate CA EKU

Key Purpose	Description
`id-kp-serverAuth`	MUST NOT be present.
`anyExtendedKeyUsage`	MUST NOT be present.
Any other value	MAY be present.

Each included Extended Key Usage key usage purpose:

1. MUST apply in the context of the public Internet (e.g. MUST NOT be for a service that is only valid in a privately managed network), unless:

DRAFT

a. the key usage purpose falls within an OID arc for which the Applicant demonstrates ownership; or,
b. the Applicant can otherwise demonstrate the right to assert the key usage purpose in a public context.

2. MUST NOT include semantics that will mislead the Relying Party about the certificate information verified by the CA, such as including a key usage purpose asserting storage on a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance.
3. MUST be verified by the Issuing CA (i.e. the Issuing CA MUST verify the Cross-Certified Subordinate CA is authorized to assert the key usage purpose).

CAs MUST NOT include additional key usage purposes unless the CA is aware of a reason for including the key usage purpose in the Certificate.

7.1.2.2.6 Cross-Certified Subordinate CA Certificate Certificate Policies

The Certificate Policies extension MUST contain at least one `PolicyInformation`. Each `PolicyInformation` MUST match the following profile:

No Policy Restrictions (Affiliated CA)

Field	Presence	Contents
`policyIdentifier`	MUST	When the Issuing CA wishes to express that there are no policy restrictions, and if the Subordinate CA is an Affiliate of the Issuing CA, then the Issuing CA MAY use the `anyPolicy` Policy Identifier, which MUST be the only `PolicyInformation` value.
`anyPolicy`	MUST	
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

Policy Restricted

Field	Presence	Contents
`policyIdentifier`	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST	The CA MUST include at least one Reserved Certificate Policy Identifier (see Section 7.1.6.1) associated with the given Subscriber Certificate type (see Section 7.1.2.7.1) transitively issued by this Certificate.

DRAFT

Field	Presence	Contents
anyPolicy	MUST NOT	The anyPolicy Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be defined by the CA and documented by the CA in its Certificate Policy and/or Certification Practice Statement.
policyQualifiers	NOT RECOMMENDED	If present, MUST contain only permitted policyQualifiers from the table below.

This Profile RECOMMENDS that the first PolicyInformation value within the Certificate Policies extension contains the Reserved Certificate Policy Identifier (see 7.1.6.1)[4]. Regardless of the order of PolicyInformation values, the Certificate Policies extension MUST include at least one Reserved Certificate Policy Identifier. If any Subscriber Certificates will chain up directly to the Certificate issued under this Certificate Profile, this Cross-Certified Subordinate CA Certificate MUST contain exactly one Reserved Certificate Policy Identifier.

Note: policyQualifiers is NOT RECOMMENDED to be present in any Certificate issued under this Certificate Profile because this information increases the size of the Certificate without providing any value to a typical Relying Party, and the information may be obtained by other means when necessary.

If the policyQualifiers is permitted and present within a PolicyInformation field, it MUST be formatted as follows:

Permitted policyQualifiers

Qualifier ID	Presence	Field Type	Contents
id-qt-cps (OID: 1.3.6.1.5.5.7.2.1)	MAY	IA5String	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

[4] Although RFC 5280 allows PolicyInformations to appear in any order, several client implementations have implemented logic that considers the policyIdentifier that matches a given filter. As such, ensuring the Reserved Certificate Policy Identifier is the first PolicyInformation reduces the risk of interoperability challenges.

7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile

This Certificate Profile MAY be used when issuing a CA Certificate that will be considered Technically Constrained, and which will not be used to issue TLS certificates directly or transitively.

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the `subject` field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.10.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.3.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
signature	

7.1.2.3.1 Technically Constrained Non-TLS Subordinate CA Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
basicConstraints	MUST	Y	See Section 7.1.2.10.4
crlDistributionPoints	MUST	N	See Section 7.1.2.11.2
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
extKeyUsage	MUST[5]	N	See Section 7.1.2.3.3

[5] While RFC 5280, Section 4.2.1.12 notes that this extension will generally only appear within end-entity certificates, these Requirements make use of this extension to further protect relying parties by limiting the scope of CA Certificates, as implemented by a number of Application Software Suppliers.

DRAFT

Extension	Presence	Critical	Description
`authorityInformationAccess`	SHOULD	N	See Section 7.1.2.10.3
`certificatePolicies`	MAY	N	See Section 7.1.2.3.2
`nameConstraints`	MAY	*[6]	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.3.2 Technically Constrained Non-TLS Subordinate CA Certificate Policies

If present, the Certificate Policies extension MUST be formatted as one of the two tables below:

No Policy Restrictions (Affiliated CA)

Field	Presence	Contents
`policyIdentifier`	MUST	When the Issuing CA wishes to express that there are no policy restrictions, the Subordinate CA MUST be an Affiliate of the Issuing CA. The Certificate Policies extension MUST contain only a single `PolicyInformation` value, which MUST contain the `anyPolicy` Policy Identifier.
`anyPolicy`	MUST	
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

Policy Restricted

Field	Presence	Contents
`policyIdentifier`	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST NOT	

[6] See Section 7.1.2.10.8 for further requirements, including regarding criticality of this extension.

DRAFT

Field	Presence	Contents
anyPolicy	MUST NOT	The anyPolicy Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be documented by the CA in its Certificate Policy and/or Certification Practice Statement.
policyQualifiers	NOT RECOMMENDED	If present, MUST contain only permitted policyQualifiers from the table below.

Permitted policyQualifiers

Qualifier ID	Presence	Field Type	Contents
id-qt-cps (OID: 1.3.6.1.5.5.7.2.1)	MAY	IA5String	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

7.1.2.3.3 Technically Constrained Non-TLS Subordinate CA Extended Key Usage

The Issuing CA MUST verify that the Subordinate CA Certificate is authorized to issue certificates for each included extended key usage purpose. Multiple, independent key purposes (e.g. id-kp-timeStamping and id-kp-codeSigning) are NOT RECOMMENDED.

Key Purpose	OID	Presence
id-kp-serverAuth	1.3.6.1.5.5.7.3.1	MUST NOT
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	MUST NOT
anyExtendedKeyUsage	2.5.29.37.0	MUST NOT
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST NOT
Any other value	-	MAY

7.1.2.4 Technically Constrained Precertificate Signing CA Certificate Profile

This Certificate Profile MUST be used when issuing a CA Certificate that will be used as a Precertificate Signing CA, as described in RFC 6962, Section 3.1. If a CA Certificate conforms to this profile, it is considered Technically Constrained.

DRAFT

A Precertificate Signing CA MUST only be used to sign Precertificates, as defined in Section 7.1.2.9. When a Precertificate Signing CA issues a Precertificate, it shall be interpreted as if the Issuing CA of the Precertificate Signing CA has issued a Certificate with a matching `tbsCertificate` of the Precertificate, after applying the modifications specified in RFC 6962, Section 3.2.

As noted in RFC 6962, Section 3.2, the `signature` field of a Precertificate is not altered as part of these modifications. As such, the Precertificate Signing CA MUST use the same signature algorithm as the Issuing CA when issuing Precertificates, and, correspondingly, MUST use a public key of the same public key algorithm as the Issuing CA, although MAY use a different CA Key Pair.

Field	**Description**
`tbsCertificate`	
`version`	MUST be v3(2)
`serialNumber`	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
`signature`	See Section 7.1.3.2
`issuer`	MUST be byte-for-byte identical to the `subject` field of the Issuing CA. See Section 7.1.4.1
`validity`	See Section 7.1.2.10.1
`subject`	See Section 7.1.2.10.2
`subjectPublicKeyInfo`	The algorithm identifier MUST be byte-for-byte identical to the algorithm identifier of the `subjectPublicKeyInfo` field of the Issuing CA. See Section 7.1.3.1
`issuerUniqueID`	MUST NOT be present
`subjectUniqueID`	MUST NOT be present
`extensions`	See Section 7.1.2.4.1
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
`signature`	

Effective 2026-03-15:

- This Certificate Profile MUST NOT be used.
- Precertificate Signing CAs MUST NOT be used to issue Precertificates.

DRAFT

7.1.2.4.1 Technically Constrained Precertificate Signing CA Extensions

Extension	Presence	Critical	Description
`authorityKeyIdentifier`	MUST	N	See Section 7.1.2.11.1
`basicConstraints`	MUST	Y	See Section 7.1.2.10.4
`certificatePolicies`	MUST	N	See Section 7.1.2.10.5
`crlDistributionPoints`	MUST	N	See Section 7.1.2.11.2
`keyUsage`	MUST	Y	See Section 7.1.2.10.7
`subjectKeyIdentifier`	MUST	N	See Section 7.1.2.11.4
`extKeyUsage`	MUST[7]	N	See Section 7.1.2.4.2
`authorityInformationAccess`	SHOULD	N	See Section 7.1.2.10.3
`nameConstraints`	MAY	*[8]	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.4.2 Technically Constrained Precertificate Signing CA Extended Key Usage

Key Purpose	OID	Presence
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST
Any other value	-	MUST NOT

7.1.2.5 Technically Constrained TLS Subordinate CA Certificate Profile

This Certificate Profile MAY be used when issuing a CA Certificate that will be considered Technically Constrained, and which will be used to issue TLS certificates directly or transitively.

[7] While RFC 5280, Section 4.2.1.12 notes that this extension will generally only appear within end-entity certificates, these Requirements make use of this extension to further protect relying parties by limiting the scope of CA Certificates, as implemented by a number of Application Software Suppliers.

[8] See Section 7.1.2.10.8 for further requirements, including regarding criticality of this extension.

DRAFT

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.10.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.5.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.5.1 Technically Constrained TLS Subordinate CA Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
basicConstraints	MUST	Y	See Section 7.1.2.10.4
certificatePolicies	MUST	N	See Section 7.1.2.10.5
crlDistributionPoints	MUST	N	See Section 7.1.2.11.2
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
extKeyUsage	MUST[9]	N	See Section 7.1.2.10.6

[9] While RFC 5280, Section 4.2.1.12 notes that this extension will generally only appear within end-entity certificates, these Requirements make use of this extension to further protect relying parties by limiting the scope of CA Certificates, as implemented by a number of Application Software Suppliers.

DRAFT

Extension	Presence	Critical	Description
`nameConstraints`	MUST	*[10]	See Section 7.1.2.5.2
`authorityInformationAccess`	SHOULD	N	See Section 7.1.2.10.3
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.5.2 Technically Constrained TLS Subordinate CA Name Constraints

For a TLS Subordinate CA to be Technically Constrained, Name Constraints extension MUST be encoded as follows. As an explicit exception from RFC 5280, this extension SHOULD be marked critical, but MAY be marked non-critical if compatibility with certain legacy applications that do not support Name Constraints is necessary.

`nameConstraints` requirements

Field	Description
`permittedSubtrees`	The `permittedSubtrees` MUST contain at least one `GeneralSubtree` for both of the `dNSName` and `iPAddress` `GeneralName` name types, UNLESS the specified `GeneralName` name type appears within the `excludedSubtrees` to exclude all names of that name type. Additionally, the `permittedSubtrees` MUST contain at least one `GeneralSubtree` of the `directoryName` `GeneralName` name type.
`GeneralSubtree`	The requirements for a `GeneralSubtree` that appears within a `permittedSubtrees`.
`base`	See following table.
`minimum`	MUST NOT be present.
`maximum`	MUST NOT be present.
`excludedSubtrees`	The `excludedSubtrees` MUST contain at least one `GeneralSubtree` for each of the `dNSName` and `iPAddress` `GeneralName` name types, unless there is an instance present of that name type in the `permittedSubtrees`. The `directoryName` name type is NOT RECOMMENDED.

[10] See Section 7.1.2.10.8 for further requirements, including regarding criticality of this extension.

DRAFT

Field	Description
GeneralSubtree	The requirements for a GeneralSubtree that appears within a permittedSubtrees.
base	See following table.
minimum	MUST NOT be present.
maximum	MUST NOT be present.

The following table contains the requirements for the GeneralName that appears within the base of a GeneralSubtree in either the permittedSubtrees or excludedSubtrees.

GeneralName requirements for the base field

Name Type	Presence	Permitted Subtrees	Excluded Subtrees	Entire Namespace Exclusion
dNSName	MUST	The CA MUST confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf. See Section 3.2.2.4.	If at least one dNSName instance is present in the permittedSubtrees, the CA MAY indicate one or more subordinate domains to be excluded.	If no dNSName instance is present in the permittedSubtrees, then the CA MUST include a zero-length dNSName to indicate no domain names are permitted.
iPAddress	MUST	The CA 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. See Section 3.2.2.5.	If at least one iPAddress instance is present in the permittedSubtrees, the CA MAY indicate one or more subdivisions of those ranges to be excluded.	If no IPv4 iPAddress is present in the permittedSubtrees, the CA MUST include an iPAddress of 8 zero octets, indicating the IPv4 range of 0.0.0.0/0 being excluded. If no IPv6 iPAddress is present in the permittedSubtrees, the CA MUST include an iPAddress of 32 zero octets, indicating the IPv6

DRAFT

Name Type	Presence	Permitted Subtrees	Excluded Subtrees	Entire Namespace Exclusion
				range of ::0/0 being excluded.
`directoryName`	MUST	The CA MUST confirm the Applicant's and/or Subsidiary's name attributes such that all certificates issued will comply with the relevant Certificate Profile (see Section 7.1.2), including Name Forms (See Section 7.1.4).	It is NOT RECOMMENDED to include values within `excludedSubtrees`.	The CA MUST include a value within `permittedSubtrees`, and as such, this does not apply. See the Excluded Subtrees requirements for more.
`otherName`	NOT RECOMMENDED	See below	See below	See below
Any other value	MUST NOT	-	-	-

Any `otherName`, if present:

1. MUST apply in the context of the public Internet, unless:
    a. the `type-id` 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.
2. MUST NOT include semantics that will mislead the Relying Party about certificate information verified by the CA.
3. MUST be DER encoded according to the relevant ASN.1 module defining the `otherName` `type-id` and `value`.

CAs SHALL NOT include additional names unless the CA is aware of a reason for including the data in the Certificate.

7.1.2.6 TLS Subordinate CA Certificate Profile

Field	Description
`tbsCertificate`	
`version`	MUST be v3(2)
`serialNumber`	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.

DRAFT

Field	Description
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.10.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.6.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.6.1 TLS Subordinate CA Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
basicConstraints	MUST	Y	See Section 7.1.2.10.4
certificatePolicies	MUST	N	See Section 7.1.2.10.5
crlDistributionPoints	MUST	N	See Section 7.1.2.11.2
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
extKeyUsage	MUST[11]	N	See Section 7.1.2.10.6
authorityInformationAccess	SHOULD	N	See Section 7.1.2.10.3
nameConstraints	MAY	*[12]	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

[11] While RFC 5280, Section 4.2.1.12 notes that this extension will generally only appear within end-entity certificates, these Requirements make use of this extension to further protect relying parties by limiting the scope of CA Certificates, as implemented by a number of Application Software Suppliers.

[12] See Section 7.1.2.10.8 for further requirements, including regarding criticality of this extension.

DRAFT

7.1.2.7 Subscriber (Server) Certificate Profile

Field	Description
`tbsCertificate`	
`version`	MUST be v3(2)
`serialNumber`	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
`signature`	See Section 7.1.3.2
`issuer`	MUST be byte-for-byte identical to the `subject` field of the Issuing CA. See Section 7.1.4.1
`validity`	
`notBefore`	A value within 48 hours of the certificate signing operation.
`notAfter`	See Section 6.3.2
`subject`	See Section 7.1.2.7.1
`subjectPublicKeyInfo`	See Section 7.1.3.1
`issuerUniqueID`	MUST NOT be present
`subjectUniqueID`	MUST NOT be present
`extensions`	See Section 7.1.2.7.6
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
`signature`	

7.1.2.7.1 Subscriber Certificate Types

There are four types of Subscriber Certificates that may be issued, which vary based on the amount of Subject Information that is included. Each of these certificate types shares a common profile, with three exceptions: the `subject` name fields that may occur, how those fields are validated, and the contents of the `certificatePolicies` extension.

Type	Description
Domain Validated (DV)	See Section 7.1.2.7.2
Individual Validated (IV)	See Section 7.1.2.7.3
Organization Validated (OV)	See Section 7.1.2.7.4
Extended Validation (EV)	See Section 7.1.2.7.5

Note: Although each Subscriber Certificate type varies in Subject Information, all Certificates provide the same level of assurance of the device identity (domain name and/or IP address).

DRAFT

7.1.2.7.2 Domain Validated

For a Subscriber Certificate to be Domain Validated, it MUST meet the following profile:

Field	Requirements
`subject`	See following table.
`certificatePolicies`	MUST be present. MUST assert the Reserved Certificate Policy Identifier of `2.23.140.1.2.1` as a `policyIdentifier`. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

All `subject` names MUST be encoded as specified in Section 7.1.4.

The following table details the acceptable `AttributeTypes` that may appear within the `type` field of an `AttributeTypeAndValue`, as well as the contents permitted within the `value` field.

Domain Validated `subject` Attributes

Attribute Name	Presence	Value	Verification
`countryName`	MAY	The two-letter ISO 3166-1 country code for the country associated with the Subject.	Section 3.2.2.3
`commonName`	NOT RECOMMENDED	If present, MUST contain a value derived from the `subjectAltName` extension according to Section 7.1.4.3.	
Any other attribute	MUST NOT	-	-

7.1.2.7.3 Individual Validated

For a Subscriber Certificate to be Individual Validated, it MUST meet the following profile:

Field	Requirements
`subject`	See following table.
`certificatePolicies`	MUST be present. MUST assert the Reserved Certificate Policy Identifier of `2.23.140.1.2.3` as a `policyIdentifier`. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

DRAFT

All `subject` names MUST be encoded as specified in Section 7.1.4.

The following table details the acceptable `AttributeTypes` that may appear within the `type` field of an `AttributeTypeAndValue`, as well as the contents permitted within the `value` field.

Individual Validated `subject` Attributes

Attribute Name	Presence	Value	Verification
`countryName`	MUST	The two-letter ISO 3166-1 country code for the country associated with the Subject. If a Country is not represented by an official ISO 3166-1 country code, the CA MUST specify the ISO 3166-1 user-assigned code of `XX`, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.	Section 3.2.3
`stateOrProvinceName`	MUST / MAY	MUST be present if `localityName` is absent, MAY be present otherwise. If present, MUST contain the Subject's state or province information.	Section 3.2.3
`localityName`	MUST / MAY	MUST be present if `stateOrProvinceName` is absent, MAY be present otherwise. If present, MUST contain the Subject's locality information.	Section 3.2.3
`postalCode`	NOT RECOMMENDED	If present, MUST contain the Subject's zip or postal information.	Section 3.2.3
`streetAddress`	NOT RECOMMENDED	If present, MUST contain the Subject's street address information. Multiple instances MAY be present.	Section 3.2.3

DRAFT

Attribute Name	Presence	Value	Verification
`organizationName`	NOT RECOMMENDED	If present, MUST contain the Subject's name and/or DBA/tradename. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations. If both are included, the DBA/tradename SHALL appear first, followed by the Subject's name in parentheses.	Section 3.2.3
`surname`	MUST	The Subject's surname.	Section 3.2.3
`givenName`	MUST	The Subject's given name.	Section 3.2.3
`organizationalUnitName`	MUST NOT	-	-
`commonName`	NOT RECOMMENDED	If present, MUST contain a value derived from the `subjectAltName` extension according to Section 7.1.4.3.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.4

In addition, `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.

7.1.2.7.4 Organization Validated

For a Subscriber Certificate to be Organization Validated, it MUST meet the following profile:

Field	Requirements
`subject`	See following table.

DRAFT

Field	Requirements
`certificatePolicies`	MUST be present. MUST assert the Reserved Certificate Policy Identifier of `2.23.140.1.2.2` as a `policyIdentifier`. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

All `subject` names MUST be encoded as specified in Section 7.1.4.

The following table details the acceptable `AttributeTypes` that may appear within the `type` field of an `AttributeTypeAndValue`, as well as the contents permitted within the `value` field.

Organization Validated `subject` Attributes

Attribute Name	Presence	Value	Verification
`domainComponent`	MAY	If present, this field MUST contain a Domain Label from a Domain Name. The `domainComponent` fields for the Domain Name MUST be in a single ordered sequence containing all Domain Labels from the Domain Name. The Domain Labels MUST be encoded in the reverse order to the on-wire representation of domain names in the DNS protocol, so that the Domain Label closest to the root is encoded first. Multiple instances MAY be present.	Section 3.2
`countryName`	MUST	The two-letter ISO 3166-1 country code for the country associated with the Subject. If a Country is not represented by an official ISO 3166-1 country code, the CA MUST specify the ISO 3166-1 user-assigned code of `XX`, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.	Section 3.2.2.1

DRAFT

Attribute Name	Presence	Value	Verification
`stateOrProvinceName`	MUST / MAY	MUST be present if `localityName` is absent, MAY be present otherwise. If present, MUST contain the Subject's state or province information.	Section 3.2.2.1
`localityName`	MUST / MAY	MUST be present if `stateOrProvinceName` is absent, MAY be present otherwise. If present, MUST contain the Subject's locality information.	Section 3.2.2.1
`postalCode`	NOT RECOMMENDED	If present, MUST contain the Subject's zip or postal information.	Section 3.2.2.1
`streetAddress`	NOT RECOMMENDED	If present, MUST contain the Subject's street address information. Multiple instances MAY be present.	Section 3.2.2.1
`organizationName`	MUST	The Subject's name and/or DBA/tradename. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name". If both are included, the DBA/tradename SHALL appear first, followed by	Section 3.2.2.2

DRAFT

Attribute Name	Presence	Value	Verification
		the Subject's name in parentheses.	
`surname`	MUST NOT	-	-
`givenName`	MUST NOT	-	-
`organizationalUnitName`	MUST NOT	-	-
`commonName`	NOT RECOMMENDED	If present, MUST contain a value derived from the `subjectAltName` extension according to Section 7.1.4.3.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.4

In addition, `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.

7.1.2.7.5 Extended Validation

For a Subscriber Certificate to be Extended Validation, it MUST comply with the Certificate Profile specified in the then-current version of the Guidelines for the Issuance and Management of Extended Validation Certificates.

In addition, it MUST meet the following profile:

Field	Requirements
`subject`	See Guidelines for the Issuance and Management of Extended Validation Certificates, Section 7.1.4.2.
`certificatePolicies`	MUST be present. MUST assert the Reserved Certificate Policy Identifier of `2.23.140.1.1` as a `policyIdentifier`. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6 and the Guidelines for the Issuance and Management of Extended Validation Certificates.

In addition, `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.

DRAFT

7.1.2.7.6 Subscriber Certificate Extensions

Extension	Presence	Critical	Description
`authorityInformationAccess`	SHOULD	N	See Section 7.1.2.7.7
`authorityKeyIdentifier`	MUST	N	See Section 7.1.2.11.1
`certificatePolicies`	MUST	N	See Section 7.1.2.7.9
`extKeyUsage`	MUST	N	See Section 7.1.2.7.10
`subjectAltName`	MUST	*	See Section 7.1.2.7.12
`nameConstraints`	MUST NOT	-	-
`keyUsage`	SHOULD	Y	See Section 7.1.2.7.11
`basicConstraints`	MAY	Y	See Section 7.1.2.7.8
`crlDistributionPoints`	*	N	See Section 7.1.2.11.2
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
`subjectKeyIdentifier`	NOT RECOMMENDED	N	See Section 7.1.2.11.4
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Notes:

- whether or not the `subjectAltName` extension should be marked Critical depends on the contents of the Certificate's `subject` field, as detailed in Section 7.1.2.7.12.
- whether or not the CRL Distribution Points extension must be present depends on 1) whether the Certificate includes an Authority Information Access extension with an `id-ad-ocsp` accessMethod and 2) the Certificate's validity period, as detailed in Section 7.1.2.11.2.

7.1.2.7.7 Subscriber Certificate Authority Information Access

If present, the `AuthorityInfoAccessSyntax` MUST contain one or more `AccessDescriptions`. Each `AccessDescription` MUST only contain a permitted `accessMethod`, as detailed below, and each `accessLocation` MUST be encoded as the specified `GeneralName` type.

The `AuthorityInfoAccessSyntax` MAY contain multiple `AccessDescriptions` with the same `accessMethod`, if permitted for that `accessMethod`. When multiple

DRAFT

AccessDescriptions are present with the same accessMethod, each accessLocation MUST be unique, and each AccessDescription MUST be ordered in priority for that accessMethod, with the most-preferred accessLocation being the first AccessDescription. No ordering requirements are given for AccessDescriptions that contain different accessMethods, provided that previous requirement is satisfied.

Access Method	Access Location	Presence	Maximum	Description
id-ad-ocsp (OID: 1.3.6.1.5.5.7.48.1)	uniformResourceIdentifier	MAY	*	A HTTP URL of the Issuing CA's OCSP responder.
id-ad-caIssuers (OID: 1.3.6.1.5.5.7.48.2)	uniformResourceIdentifier	SHOULD	*	A HTTP URL of the Issuing CA's certificate.
Any other value	-	MUST NOT	-	No other accessMethods may be used.

7.1.2.7.8 Subscriber Certificate Basic Constraints

Field	Description
cA	MUST be FALSE
pathLenConstraint	MUST NOT be present

7.1.2.7.9 Subscriber Certificate Certificate Policies

If present, the Certificate Policies extension MUST contain at least one PolicyInformation. Each PolicyInformation MUST match the following profile:

Field	Presence	Contents
policyIdentifier	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST	The Reserved Certificate Policy Identifier (see Section 7.1.6.1) associated with the given Subscriber Certificate type (see Section 7.1.2.7.1).
anyPolicy	MUST NOT	The anyPolicy Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be defined and documented in the CA's Certificate Policy and/or Certification Practice Statement.
policyQualifiers	NOT RECOMMENDED	If present, MUST contain only permitted policyQualifiers from the table below.

DRAFT

This Profile RECOMMENDS that the first `PolicyInformation` value within the Certificate Policies extension contains the Reserved Certificate Policy Identifier (see 7.1.6.1)[13]. Regardless of the order of `PolicyInformation` values, the Certificate Policies extension MUST contain exactly one Reserved Certificate Policy Identifier.

Permitted `policyQualifiers`

Qualifier ID	Presence	Field Type	Contents
`id-qt-cps` (OID: 1.3.6.1.5.5.7.2.1)	MAY	`IA5String`	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

7.1.2.7.10 Subscriber Certificate Extended Key Usage

Key Purpose	OID	Presence
`id-kp-serverAuth`	1.3.6.1.5.5.7.3.1	MUST
`id-kp-clientAuth`	1.3.6.1.5.5.7.3.2	MAY
`id-kp-codeSigning`	1.3.6.1.5.5.7.3.3	MUST NOT
`id-kp-emailProtection`	1.3.6.1.5.5.7.3.4	MUST NOT
`id-kp-timeStamping`	1.3.6.1.5.5.7.3.8	MUST NOT
`id-kp-OCSPSigning`	1.3.6.1.5.5.7.3.9	MUST NOT
`anyExtendedKeyUsage`	2.5.29.37.0	MUST NOT
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST NOT
Any other value	-	NOT RECOMMENDED

7.1.2.7.11 Subscriber Certificate Key Usage

The acceptable Key Usage values vary based on whether the Certificate's `subjectPublicKeyInfo` identifies an RSA public key or an ECC public key. CAs MUST ensure the Key Usage is appropriate for the Certificate Public Key.

---

[13] Although RFC 5280 allows `PolicyInformation`s to appear in any order, several client implementations have implemented logic that considers the `policyIdentifier` that matches a given filter. As such, ensuring the Reserved Certificate Policy Identifier is the first `PolicyInformation` reduces the risk of interoperability challenges.

DRAFT

Key Usage for RSA Public Keys

Key Usage	Permitted	Required
digitalSignature	Y	SHOULD
nonRepudiation	N	–
keyEncipherment	Y	MAY
dataEncipherment	Y	NOT RECOMMENDED
keyAgreement	N	–
keyCertSign	N	–
cRLSign	N	–
encipherOnly	N	–
decipherOnly	N	–

Note: At least one Key Usage MUST be set for RSA Public Keys. The digitalSignature bit is REQUIRED for use with modern protocols, such as TLS 1.3, and secure ciphersuites, while the keyEncipherment bit MAY be asserted to support older protocols, such as TLS 1.2, when using insecure ciphersuites. Subscribers MAY wish to ensure key separation to limit the risk from such legacy protocols, and thus a CA MAY issue a Subscriber certificate that only asserts the keyEncipherment bit. For most Subscribers, the digitalSignature bit is sufficient, while Subscribers that want to mix insecure and secure ciphersuites with the same algorithm may choose to assert both digitalSignature and keyEncipherment within the same certificate, although this is NOT RECOMMENDED. The dataEncipherment bit is currently permitted, although setting it is NOT RECOMMENDED, as it is a Pending Prohibition (https://github.com/cabforum/servercert/issues/384).

Key Usage for ECC Public Keys

Key Usage	Permitted	Required
digitalSignature	Y	MUST
nonRepudiation	N	–
keyEncipherment	N	–
dataEncipherment	N	–
keyAgreement	Y	NOT RECOMMENDED
keyCertSign	N	–
cRLSign	N	–
encipherOnly	N	–
decipherOnly	N	–

Note: The keyAgreement bit is currently permitted, although setting it is NOT RECOMMENDED, as it is a Pending Prohibition (https://github.com/cabforum/servercert/issues/384).

DRAFT

7.1.2.7.12 Subscriber Certificate Subject Alternative Name

For Subscriber Certificates, the Subject Alternative Name MUST be present and MUST contain at least one `dNSName` or `iPAddress` `GeneralName`. See below for further requirements about the permitted fields and their validation requirements.

If the `subject` field of the certificate is an empty SEQUENCE, this extension MUST be marked critical, as specified in RFC 5280, Section 4.2.1.6. Otherwise, this extension MUST NOT be marked critical.

`GeneralName` within a `subjectAltName` extension

Name Type	**Permitted**	**Validation**
`otherName`	N	-
`rfc822Name`	N	-
`dNSName`	Y	The entry MUST contain either a Fully-Qualified Domain Name or Wildcard Domain Name that the CA has validated in accordance with Section 3.2.2.4. Wildcard Domain Names MUST be validated for consistency with Section 3.2.2.6. The entry MUST NOT contain an Internal 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 MUST be composed entirely of P-Labels or Non-Reserved LDH Labels joined together by a U+002E FULL STOP (“.”) character. The zero-length Domain Label representing the root zone of the Internet Domain Name System MUST NOT be included (e.g. “example.com” MUST be encoded as “example.com” and MUST NOT be encoded as “example.com.”).
`x400Address`	N	-
`directoryName`	N	-
`ediPartyName`	N	-
`uniformResourceIdentifier`	N	-
`iPAddress`	Y	The entry MUST contain the IPv4 or IPv6 address that the CA has confirmed the Applicant controls or has been granted the right to use through a method specified in

DRAFT

Name Type	Permitted	Validation
		Section 3.2.2.5. The entry MUST NOT contain a Reserved IP Address.
registeredID	N	-

Note: As an explicit exception from RFC 5280, P-Labels are permitted to not conform to IDNA 2003. These Requirements allow for the inclusion of P-Labels that do not conform with IDNA 2003 to support newer versions of the Unicode character repertoire, among other improvements to the various IDNA standards.

7.1.2.8 OCSP Responder Certificate Profile

If the Issuing CA does not directly sign OCSP responses, it MAY make use of an OCSP Authorized Responder, as defined by RFC 6960, Section 4.2.2.2. The Issuing CA of the Responder MUST be the same as the Issuing CA for the Certificates it provides responses for.

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.8.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.8.2
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.8.1 OCSP Responder Validity

Field	Minimum	Maximum
notBefore	One day prior to the time of signing	The time of signing
notAfter	The time of signing	Unspecified

DRAFT

7.1.2.8.2 OCSP Responder Extensions

Extension	Presence	Critical	Description
`authorityKeyIdentifier`	MUST	N	See Section 7.1.2.11.1
`extKeyUsage`	MUST	-	See Section 7.1.2.8.5
`id-pkix-ocsp-nocheck`	MUST	N	See Section 7.1.2.8.6
`keyUsage`	MUST	Y	See Section 7.1.2.8.7
`basicConstraints`	MAY	Y	See Section 7.1.2.8.4
`nameConstraints`	MUST NOT	-	-
`subjectAltName`	MUST NOT	-	-
`subjectKeyIdentifier`	SHOULD	N	See Section 7.1.2.11.4
`authorityInformationAccess`	NOT RECOMMENDED	N	See Section 7.1.2.8.3
`certificatePolicies`	SHOULD NOT	N	See Section 7.1.2.8.8
`crlDistributionPoints`	MUST NOT	N	See Section 7.1.2.11.2
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.8.3 OCSP Responder Authority Information Access

For OCSP Responder 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, 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`.

DRAFT

Access Method	Access Location	Presence	Maximum	Description
id-ad-ocsp (OID: 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.

7.1.2.8.4 OCSP Responder Basic Constraints

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.

7.1.2.8.5 OCSP Responder Extended Key Usage

Key Purpose	OID	Presence
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	MUST
Any other value	-	MUST NOT

7.1.2.8.6 OCSP Responder id-pkix-ocsp-nocheck

The CA MUST include the id-pkix-ocsp-nocheck extension (OID: 1.3.6.1.5.5.7.48.1.5).

This extension MUST have an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6960, Section 4.2.2.2.1.

7.1.2.8.7 OCSP Responder Key Usage

Key Usage	Permitted	Required
digitalSignature	Y	Y
nonRepudiation	N	-

DRAFT

Key Usage	Permitted	Required
keyEncipherment	N	–
dataEncipherment	N	–
keyAgreement	N	–
keyCertSign	N	–
cRLSign	N	–
encipherOnly	N	–
decipherOnly	N	–

7.1.2.8.8 OCSP Responder Certificate Policies

If present, the Certificate Policies extension MUST contain at least one `PolicyInformation`. Each `PolicyInformation` MUST match the following profile:

Permitted `policyQualifiers`

Field	Presence	Contents
`policyIdentifier`	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	NOT RECOMMENDED	
`anyPolicy`	NOT RECOMMENDED	
Any other identifier	NOT RECOMMENDED	If present, MUST be defined by the CA and documented by the CA in its Certificate Policy and/or Certification Practice Statement.
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

Qualifier ID	Presence	Field Type	Contents
`id-qt-cps` (OID: 1.3.6.1.5.5.7.2.1)	MAY	`IA5String`	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

DRAFT

Note: Because the Certificate Policies extension may be used to restrict the applicable usages for a Certificate, incorrect policies may result in OCSP Responder Certificates that fail to successfully validate, resulting in invalid OCSP Responses. Including the `anyPolicy` policy can reduce this risk, but add to client processing complexity and interoperability issues.

7.1.2.9 Precertificate Profile

A Precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC 6962. A Precertificate appears structurally identical to a Certificate, with the exception of a special critical poison extension in the `extensions` field, with the OID of 1.3.6.1.4.1.11129.2.4.3. This extension ensures that the Precertificate will not be accepted as a Certificate by clients conforming to RFC 5280. The existence of a signed Precertificate can be treated as evidence of a corresponding Certificate also existing, as the signature represents a binding commitment by the CA that it may issue such a Certificate.

A Precertificate is created after a CA has decided to issue a Certificate, but prior to the actual signing of the Certificate. The CA MAY construct and sign a Precertificate corresponding to the Certificate, for purposes of submitting to Certificate Transparency Logs. The CA MAY use the returned Signed Certificate Timestamps to then alter the Certificate's `extensions` field, adding a Signed Certificate Timestamp List, as defined in Section 7.1.2.11.3 and as permitted by the relevant profile, prior to signing the Certificate.

Once a Precertificate is signed, relying parties are permitted to treat this as a binding commitment from the CA of the intent to issue a corresponding Certificate, or more commonly, that a corresponding Certificate exists. A Certificate is said to be corresponding to a Precertificate based upon the value of the `tbsCertificate` contents, as transformed by the process defined in RFC 6962, Section 3.2.

This profile describes the transformations that are permitted to a Certificate to construct a Precertificate. CAs MUST NOT issue a Precertificate unless they are willing to issue a corresponding Certificate, regardless of whether they have done so. Similarly, a CA MUST NOT issue a Precertificate unless the corresponding Certificate conforms to these Baseline Requirements, regardless of whether the CA signs the corresponding Certificate.

A Precertificate may be issued either directly by the Issuing CA or, when issued prior to 2026-03-15, by a Technically Constrained Precertificate Signing CA, as defined in Section 7.1.2.4. If issued by a Precertificate Signing CA, then in addition to the precertificate poison and signed certificate timestamp list extensions, the Precertificate issuer field and, if present, `authorityKeyIdentifier` extension, may differ from the Certificate, as described below.

DRAFT

When the Precertificate is issued directly by the Issuing CA

Field	Description
`tbsCertificate`	
`version`	Encoded value MUST be byte-for-byte identical to the `version` field of the Certificate
`serialNumber`	Encoded value MUST be byte-for-byte identical to the `serialNumber` field of the Certificate
`signature`	Encoded value MUST be byte-for-byte identical to the `signature` field of the Certificate
`issuer`	Encoded value MUST be byte-for-byte identical to the `issuer` field of the Certificate
`validity`	Encoded value MUST be byte-for-byte identical to the `validity` field of the Certificate
`subject`	Encoded value MUST be byte-for-byte identical to the `subject` field of the Certificate
`subjectPublicKeyInfo`	Encoded value MUST be byte-for-byte identical to the `subjectPublicKeyInfo` field of the Certificate
`issuerUniqueID`	Encoded value MUST be byte-for-byte identical to the `issuerUniqueID` field of the Certificate, or omitted if omitted in the Certificate
`subjectUniqueID`	Encoded value MUST be byte-for-byte identical to the `subjectUniqueID` field of the Certificate, or omitted if omitted in the Certificate
`extensions`	See Section 7.1.2.9.1
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
`signature`	

When the Precertificate is issued by a Precertificate Signing CA on behalf of an Issuing CA

Field	Description
`tbsCertificate`	
`version`	Encoded value MUST be byte-for-byte identical to the `version` field of the Certificate
`serialNumber`	Encoded value MUST be byte-for-byte identical to the `serialNumber` field of the Certificate
`signature`	Encoded value MUST be byte-for-byte identical to the `signature` field of the Certificate
`issuer`	Encoded value MUST be byte-for-byte identical to the `subject` field of the Precertificate Signing CA Certificate

DRAFT

Field	Description
validity	Encoded value MUST be byte-for-byte identical to the validity field of the Certificate
subject	Encoded value MUST be byte-for-byte identical to the subject field of the Certificate
subjectPublicKeyInfo	Encoded value MUST be byte-for-byte identical to the subjectPublicKeyInfo field of the Certificate
issuerUniqueID	Encoded value MUST be byte-for-byte identical to the issuerUniqueID field of the Certificate, or omitted if omitted in the Certificate
subjectUniqueID	Encoded value MUST be byte-for-byte identical to the subjectUniqueID field of the Certificate, or omitted if omitted in the Certificate
extensions	See Section 7.1.2.9.2
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

Note: This profile requires that the serialNumber field of the Precertificate be identical to that of the corresponding Certificate. RFC 5280, Section 4.1.2.2 requires that the serialNumber of certificates be unique. For the purposes of this document, a Precertificate shall not be considered a "certificate" subject to that requirement, and thus may have the same serialNumber of the corresponding Certificate. However, this does not permit two Precertificates to share the same serialNumber, unless they correspond to the same Certificate, as this would otherwise indicate there are two corresponding Certificates that share the same serialNumber.

7.1.2.9.1 Precertificate Profile Extensions - Directly Issued

These extensions apply in the context of a Precertificate directly issued from a CA, and not from a Precertificate Signing CA Certificate, as defined in Section 7.1.2.4.

Extension	Presence	Critical	Description
Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)	MUST	Y	See Section 7.1.2.9.3
Signed Certificate Timestamp List	MUST NOT	-	
Any other extension	*	*	The order, criticality, and encoded values of all other extensions MUST be byte-for-byte identical to the extensions field of the Certificate

Note: This requirement is expressing that if the Precertificate Poison extension is removed from the Precertificate, and the Signed Certificate Timestamp List is removed from the certificate, the contents of the `extensions` field MUST be byte-for-byte identical to the Certificate.

7.1.2.9.2 Precertificate Profile Extensions - Precertificate CA Issued

These extensions apply in the context of a Precertificate from a Precertificate Signing CA Certificate, as defined in Section 7.1.2.4. For such Precertificates, the `authorityKeyIdentifier`, if present in the Certificate, is modified in the Precertificate, as described in RFC 6962, Section 3.2.

Extension	Presence	Critical	Description
Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)	MUST	Y	See Section 7.1.2.9.3
`authorityKeyIdentifier`	*	*	See Section 7.1.2.9.4
Signed Certificate Timestamp List	MUST NOT	-	
Any other extension	*	*	The order, criticality, and encoded values of all other extensions MUST be byte-for-byte identical to the `extensions` field of the Certificate

7.1.2.9.3 Precertificate Poison

The Precertificate MUST contain the Precertificate Poison extension (OID: 1.3.6.1.4.1.11129.2.4.3).

This extension MUST have an `extnValue OCTET STRING` which is exactly the hex-encoded bytes `0500`, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

7.1.2.9.4 Precertificate Authority Key Identifier

For Precertificates issued by a Precertificate Signing CA, the contents of the `authorityKeyIdentifier` extension MUST be one of the following:

1. SHOULD be as defined in the profile below, or;
2. MAY be byte-for-byte identical with the contents of the `authorityKeyIdentifier` extension of the corresponding Certificate.

Field	Description
`keyIdentifier`	MUST be present. MUST be identical to the `subjectKeyIdentifier` field of the Precertificate Signing CA Certificate

DRAFT

Field	Description
authorityCertIssuer	MUST NOT be present
authorityCertSerialNumber	MUST NOT be present

Note: RFC 6962 describes how the authorityKeyIdentifier present on a Precertificate is transformed to contain the value of the Precertificate Signing CA's authorityKeyIdentifier extension (i.e. reflecting the actual issuer certificate's keyIdentifier), thus matching the corresponding Certificate when verified by clients. These Baseline Requirements RECOMMEND the use of the Precertificate Signing CA's keyIdentifier in Precertificates issued by it in order to ensure consistency between the subjectKeyIdentifier and authorityKeyIdentifier of all certificates in the chain. Although RFC 5280 does not strictly require such consistency, a number of client implementations enforce such consistency for Certificates, and this avoids any risks from Certificate Transparency Logs incorrectly implementing such checks.

7.1.2.10 Common CA Fields

This section contains several fields that are common among multiple CA Certificate profiles. However, these fields may not be common among all CA Certificate profiles. Before issuing a certificate, the CA MUST ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.10.1 CA Certificate Validity

Field	Minimum	Maximum
notBefore	One day prior to the time of signing	The time of signing
notAfter	The time of signing	Unspecified

7.1.2.10.2 CA Certificate Naming

All subject names MUST be encoded as specified in Section 7.1.4.

The following table details the acceptable AttributeTypes that may appear within the type field of an AttributeTypeAndValue, as well as the contents permitted within the value field.

Attribute Name	Presence	Value	Verification
countryName	MUST	The two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.	Section 3.2.2.3

Attribute Name	Presence	Value	Verification
stateOrProvinceName	MAY	If present, the CA's state or province information.	Section 3.2.2.1
localityName	MAY	If present, the CA's locality.	Section 3.2.2.1
postalCode	MAY	If present, the CA's zip or postal information.	Section 3.2.2.1
streetAddress	MAY	If present, the CA's street address. Multiple instances MAY be present.	Section 3.2.2.1
organizationName	MUST	The CA's name or DBA. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name".	Section 3.2.2.2
organizationalUnitName	This attribute MUST NOT be included in Root CA Certificates defined in Section 7.1.2.1 or TLS Subordinate CA Certificates defined in Section 7.1.2.5 or Technically-Constrained TLS Subordinate CA Certificates defined in Section 7.1.2.6. This attribute	-	-

DRAFT

Attribute Name	Presence	Value	Verification
	SHOULD NOT be included in other types of CA Certificates.		
commonName	MUST	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.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.4

7.1.2.10.3 CA Certificate Authority Information Access

If present, the AuthorityInfoAccessSyntax MUST contain one or more AccessDescriptions. Each AccessDescription MUST only contain a permitted accessMethod, as detailed below, and each accessLocation MUST be encoded as the specified GeneralName type.

The AuthorityInfoAccessSyntax MAY contain multiple AccessDescriptions with the same accessMethod, if permitted for that accessMethod. When multiple AccessDescriptions are present with the same accessMethod, each accessLocation MUST be unique, and each AccessDescription MUST be ordered in priority for that accessMethod, with the most-preferred accessLocation being the first AccessDescription. No ordering requirements are given for AccessDescriptions that contain different accessMethods, provided that previous requirement is satisfied.

Access Method	Access Location	Presence	Maximum	Description
id-ad-ocsp (OID: 1.3.6.1.5.5.7.48.1)	uniformResourceIdentifier	MAY	*	A HTTP URL of the Issuing CA's OCSP responder.
id-ad-caIssuers (OID: 1.3.6.1.5.5.7.48.2)	uniformResourceIdentifier	MAY	*	A HTTP URL of the Issuing CA's certificate.
Any other value	-	MUST NOT	-	No other accessMethods may be used.

DRAFT

7.1.2.10.4 CA Certificate Basic Constraints

Field	Description
`cA`	MUST be set TRUE
`pathLenConstraint`	MAY be present

7.1.2.10.5 CA Certificate Certificate Policies

If present, the Certificate Policies extension MUST contain at least one `PolicyInformation`. Each `PolicyInformation` MUST match the following profile:

No Policy Restrictions (Affiliated CA)

Field	Presence	Contents
`policyIdentifier`	MUST	When the Issuing CA wishes to express that there are no policy restrictions, and if the Subordinate CA is an Affiliate of the Issuing CA, then the Issuing CA MAY use the `anyPolicy` Policy Identifier, which MUST be the only `PolicyInformation` value.
`anyPolicy`	MUST	
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

Policy Restricted

Field	Presence	Contents
`policyIdentifier`	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST	The CA MUST include exactly one Reserved Certificate Policy Identifier (see Section 7.1.6.1) associated with the given Subscriber Certificate type (see Section 7.1.2.7.1) directly or transitively issued by this Certificate.
`anyPolicy`	MUST NOT	The `anyPolicy` Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be defined by the CA and documented by the CA in its Certificate Policy and/or Certification Practice Statement.
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

DRAFT

The Policy Restricted profile RECOMMENDS that the first `PolicyInformation` value within the Certificate Policies extension contains the Reserved Certificate Policy Identifier (see 7.1.6.1)[14]. Regardless of the order of `PolicyInformation` values, the Certificate Policies extension MUST contain exactly one Reserved Certificate Policy Identifier.

Note: `policyQualifiers` is NOT RECOMMENDED to be present in any Certificate issued under this Certificate Profile because this information increases the size of the Certificate without providing any value to a typical Relying Party, and the information may be obtained by other means when necessary.

If the `policyQualifiers` is permitted and present within a `PolicyInformation` field, it MUST be formatted as follows:

Permitted `policyQualifiers`

Qualifier ID	Presence	Field Type	Contents
`id-qt-cps` (OID: 1.3.6.1.5.5.7.2.1)	MAY	`IA5String`	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

7.1.2.10.6 CA Certificate Extended Key Usage

Key Purpose	OID	Presence
`id-kp-serverAuth`	1.3.6.1.5.5.7.3.1	MUST
`id-kp-clientAuth`	1.3.6.1.5.5.7.3.2	MAY
`id-kp-codeSigning`	1.3.6.1.5.5.7.3.3	MUST NOT
`id-kp-emailProtection`	1.3.6.1.5.5.7.3.4	MUST NOT
`id-kp-timeStamping`	1.3.6.1.5.5.7.3.8	MUST NOT
`id-kp-OCSPSigning`	1.3.6.1.5.5.7.3.9	MUST NOT
`anyExtendedKeyUsage`	2.5.29.37.0	MUST NOT
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST NOT

[14] Although RFC 5280 allows `PolicyInformations` to appear in any order, several client implementations have implemented logic that considers the `policyIdentifier` that matches a given filter. As such, ensuring the Reserved Certificate Policy Identifier is the first `PolicyInformation` reduces the risk of interoperability challenges.

Key Purpose	OID	Presence
Any other value	-	NOT RECOMMENDED

7.1.2.10.7 CA Certificate Key Usage

Key Usage	Permitted	Required
`digitalSignature`	Y	N[15]
`nonRepudiation`	N	–
`keyEncipherment`	N	–
`dataEncipherment`	N	–
`keyAgreement`	N	–
`keyCertSign`	Y	Y
`cRLSign`	Y	Y
`encipherOnly`	N	–
`decipherOnly`	N	–

7.1.2.10.8 CA Certificate Name Constraints

If present, the Name Constraints extension MUST be encoded as follows. As an explicit exception from RFC 5280, this extension SHOULD be marked critical, but MAY be marked non-critical if compatibility with certain legacy applications that do not support Name Constraints is necessary.

`nameConstraints` requirements

Field	Description
`permittedSubtrees`	
`GeneralSubtree`	The requirements for a `GeneralSubtree` that appears within a `permittedSubtrees`.
`base`	See following table.
`minimum`	MUST NOT be present.
`maximum`	MUST NOT be present.
`excludedSubtrees`	
`GeneralSubtree`	The requirements for a `GeneralSubtree` that appears within a `permittedSubtrees`.
`base`	See following table.
`minimum`	MUST NOT be present.

[15] If a CA Certificate does not assert the `digitalSignature` bit, the CA Private Key MUST NOT be used to sign an OCSP Response. See Section 7.3 for more information.

Field	Description
maximum	MUST NOT be present.

The following table contains the requirements for the GeneralName that appears within the base of a GeneralSubtree in either the permittedSubtrees or excludedSubtrees.

GeneralName requirements for the base field

Name Type	Presence	Permitted Subtrees	Excluded Subtrees
dNSName	MAY	The CA MUST confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf. See Section 3.2.2.4.	If at least one dNSName instance is present in the permittedSubtrees, the CA MAY indicate one or more subordinate domains to be excluded.
iPAddress	MAY	The CA 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. See Section 3.2.2.5.	If at least one iPAddress instance is present in the permittedSubtrees, the CA MAY indicate one or more subdivisions of those ranges to be excluded.
directoryName	MAY	The CA MUST confirm the Applicant's and/or Subsidiary's name attributes such that all certificates issued will comply with the relevant Certificate Profile (see Section 7.1.2), including Name Forms (See Section 7.1.4).	It is NOT RECOMMENDED to include values within excludedSubtrees.

DRAFT

Name Type	Presence	Permitted Subtrees	Excluded Subtrees
`rfc822Name`	NOT RECOMMENDED	The CA MAY constrain to a mailbox, a particular host, or any address within a domain, as specified within RFC 5280, Section 4.2.1.10. For each host, domain, or Domain portion of a Mailbox (as specified within RFC 5280, Section 4.2.1.6), the CA MUST confirm that the Applicant has registered the domain or has been authorized by the domain registrant to act on the registrant's behalf. See Section 3.2.2.4.	If at least one `rfc822Name` instance is present in the `permittedSubtrees`, the CA MAY indicate one or more mailboxes, hosts, or domains to be excluded.
`otherName`	NOT RECOMMENDED	See below	See below
Any other value	NOT RECOMMENDED	-	-

Any `otherName`, if present:

1. MUST apply in the context of the public Internet, unless:
    a. the `type-id` 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.
2. MUST NOT include semantics that will mislead the Relying Party about certificate information verified by the CA.
3. MUST be DER encoded according to the relevant ASN.1 module defining the `otherName` `type-id` and `value`.

CAs SHALL NOT include additional names unless the CA is aware of a reason for including the data in the Certificate.

7.1.2.11 Common Certificate Fields

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

DRAFT

Before issuing a certificate, the CA MUST ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.11.1 Authority Key Identifier

Field	Description
`keyIdentifier`	MUST be present. MUST be identical to the `subjectKeyIdentifier` field of the Issuing CA.
`authorityCertIssuer`	MUST NOT be present
`authorityCertSerialNumber`	MUST NOT be present

7.1.2.11.2 CRL Distribution Points

The CRL Distribution Points extension MUST be present in:

- Subordinate CA Certificates; and
- 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 SHOULD NOT be present in:

- Root CA Certificates.

The CRL Distribution Points extension is OPTIONAL in:

- Short-lived Subscriber Certificates.

The CRL Distribution Points extension MUST NOT be present in:

- OCSP Responder 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:

`DistributionPoint` profile

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.

7.1.2.11.3 Signed Certificate Timestamp List

If present, the Signed Certificate Timestamp List extension contents MUST be an `OCTET STRING` containing the encoded `SignedCertificateTimestampList`, as specified in RFC 6962, Section 3.3.

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

7.1.2.11.4 Subject Key Identifier

If present, the `subjectKeyIdentifier` MUST be set as defined within RFC 5280, Section 4.2.1.2. The CA MUST generate a `subjectKeyIdentifier` that is unique within the scope of all Certificates it has issued for each unique public key (the `subjectPublicKeyInfo` field of the `tbsCertificate`). For example, CAs may generate the subject key identifier using an algorithm derived from the public key, or may generate a sufficiently-large unique number, such as by using a CSPRNG.

7.1.2.11.5 Other Extensions

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

1. MUST apply in the context of the public Internet, unless:
    a. the extension OID 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.
2. MUST NOT include semantics that will mislead the Relying Party about certificate information verified by the CA (such as including an extension that indicates a Private Key is stored on a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).
3. MUST be DER encoded according to the relevant ASN.1 module defining the extension and extension values.

CAs SHALL NOT include additional extensions or values unless the CA is aware of a reason for including the data in the Certificate.

DRAFT

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

The CA 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. The CA 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

The CA SHALL indicate an ECDSA key using the `id-ecPublicKey` (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters MUST 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`.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a CA Private Key MUST conform to these requirements 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

DRAFT

- The `signatureAlgorithm` field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

The CA 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:

  ```
  304106092a864886f70d01010a3034a00f300d060960864801650304020105
  00a11c301a06092a864886f70d010108300d060960864801650304020105
  00a203020120
  ```

- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes:

  Encoding:

  ```
  304106092a864886f70d01010a3034a00f300d060960864801650304020205
  00a11c301a06092a864886f70d010108300d060960864801650304020205
  00a203020130
  ```

- RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:

  Encoding:

  ```
  304106092a864886f70d01010a3034a00f300d060960864801650304020305
  00a11c301a06092a864886f70d010108300d060960864801650304020305
  00a203020140
  ```

Until 2026-09-15, the CA MAY use the following signature algorithm and encoding if all of the following conditions are met:

DRAFT

- 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 a CA to sign a Precertificate with this encoding.

- RSASSA-PKCS1-v1_5 with SHA-1:

  Encoding: `300d06092a864886f70d0101050500`

Prior to 2026-09-15, the CA SHALL revoke any unexpired Subordinate CA Certificate that contains `RSASSA-PKCS1-v1_5 with SHA-1` within the Certificate.

DRAFT

7.1.3.2.2 ECDSA

The CA 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`.

7.1.4 Name Forms

This section details encoding rules that apply to all Certificates issued by a CA. Further restrictions may be specified within Section 7.1.2, but these restrictions do not supersede these requirements.

7.1.4.1 Name Encoding

The following requirements apply to all Certificates listed in Section 7.1.2. Specifically, this includes Technically Constrained Non-TLS Subordinate CA Certificates, as defined in Section 7.1.2.3, but does not include certificates issued by such CA Certificates, as they are out of scope of these Baseline Requirements.

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.

When encoding a `Name`, the CA SHALL ensure that:

- Each `Name` MUST contain an `RDNSequence`.
- Each `RelativeDistinguishedName` MUST contain exactly one `AttributeTypeAndValue`.
- Each `RelativeDistinguishedName`, if present, is encoded within the `RDNSequence` in the order that it appears in Section 7.1.4.2.

DRAFT

    - For example, a RelativeDistinguishedName that contains a countryName AttributeTypeAndValue pair MUST be encoded within the RDNSequence before a RelativeDistinguishedName that contains a stateOrProvinceName AttributeTypeAndValue.
- Each Name MUST NOT contain more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames unless explicitly allowed in these Requirements.

Note: Section 7.1.2.2.2 provides an exception to the above Name encoding requirements when issuing a Cross-Certified Subordinate CA Certificate, as described within that section.

7.1.4.2 Subject Attribute Encoding

This document defines requirements for the content and validation of a number of attributes that may appear within the subject field of a tbsCertificate. CAs SHALL NOT include these attributes unless their content has been validated as specified by, and only if permitted by, the relevant certificate profile specified within Section 7.1.2.

CAs that include attributes in the Certificate subject field that are listed in the table below SHALL encode those attributes in the relative order as they appear in the table and follow the specified encoding requirements for the attribute.

Encoding and Order Requirements for Selected Attributes

Attribute	OID	Specification	Encoding Requirements	Max Length*
domainComponent	0.9.2342.19200300.100.1.25	RFC 4519	MUST use IA5String	63
countryName	2.5.4.6	RFC 5280	MUST use PrintableString	2
stateOrProvinceName	2.5.4.8	RFC 5280	MUST use UTF8String or PrintableString	128
localityName	2.5.4.7	RFC 5280	MUST use UTF8String or PrintableString	128
postalCode	2.5.4.17	X.520	MUST use UTF8String or PrintableString	40
streetAddress	2.5.4.9	X.520	MUST use UTF8String or PrintableString	128
organizationName	2.5.4.10	RFC 5280	MUST use UTF8String or PrintableString	64

DRAFT

Attribute	OID	Specification	Encoding Requirements	Max Length*
surname	2.5.4.4	RFC 5280	MUST use UTF8String or PrintableString	64[16]
givenName	2.5.4.42	RFC 5280	MUST use UTF8String or PrintableString	64[17]
organizationalUnitName	2.5.4.11	RFC 5280	MUST use UTF8String or PrintableString	64
commonName	2.5.4.3	RFC 5280	MUST use UTF8String or PrintableString	64

* **Note**: ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits.

CAs that include attributes in the Certificate subject field that are listed in the table below SHALL follow the specified encoding requirements for the attribute.

Encoding Requirements for Selected Attributes

Attribute	OID	Specification	Encoding Requirements	Max Length*
businessCategory	2.5.4.15	X.520	MUST use UTF8String or PrintableString	128
jurisdictionCountry	1.3.6.1.4.1.311.60.2.1.3	Guidelines for the Issuance and Management of Extended Validation Certificates	MUST use PrintableString	2
jurisdictionStateOrProvince	1.3.6.1.4.1.311.60.2.1.2	Guidelines for the Issuance and Management of Extended Validation Certificates	MUST use UTF8String or PrintableString	128

[16] **Note**: Although RFC 5280 specifies the upper bound as 32,768 characters, this was a transcription error from X.520 (08/2005). The effective (interoperable) upper bound is 64 characters.

[17] **Note**: Although RFC 5280 specifies the upper bound as 32,768 characters, this was a transcription error from X.520 (08/2005). The effective (interoperable) upper bound is 64 characters.

DRAFT

Attribute	OID	Specification	Encoding Requirements	Max Length*
jurisdictionLocality	1.3.6.1.4.1.311.60.2.1.1	Guidelines for the Issuance and Management of Extended Validation Certificates	MUST use UTF8String or PrintableString	128
serialNumber	2.5.4.5	RFC 5280	MUST use PrintableString	64
organizationIdentifier	2.5.4.97	X.520	MUST use UTF8String or PrintableString	None

* **Note**: ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits.

7.1.4.3 Subscriber Certificate Common Name Attribute

If present, this attribute MUST contain exactly one entry that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.2.7.12). 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.

7.1.4.4 Other Subject Attributes

When explicitly stated as permitted by the relevant certificate profile specified within Section 7.1.2, CAs MAY include additional attributes within the AttributeTypeAndValue beyond those specified in Section 7.1.4.2.

Before including such an attribute, the CA SHALL:

- Document the attributes within Section 7.1.4 of their CP or CPS, along with the applicable validation practices.
- Ensure that the contents contain information that has been verified by the CA, independent of the Applicant.

DRAFT

7.1.5 Name constraints

See Sections 7.1.2.5.2 Technically Constrained TLS Subordinate CA Name Constraints and 7.1.2.10.8 CA Certificate Name Constraints.

7.1.6 Certificate policy object identifier

7.1.6.1 Reserved Certificate Policy Identifiers

The following Certificate Policy identifiers are reserved for use by CAs as an optional means of asserting that a Certificate complies with these Requirements.

```
{joint-iso-itu-t(2) international-organizations(23) ca-browser-
forum(140) certificate-policies(1) baseline-requirements(2) domain-
validated(1)} (2.23.140.1.2.1)

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

{joint-iso-itu-t(2) international-organizations(23) ca-browser-
forum(140) certificate-policies(1) baseline-requirements(2)
individual-validated(3)} (2.23.140.1.2.3)

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

7.1.7 Usage of Policy Constraints extension

7.1.8 Policy qualifiers syntax and semantics

7.1.9 Processing semantics for the critical Certificate Policies extension

7.2 CRL profile

Prior to 2024-03-15, the CA SHALL issue CRLs in accordance with the profile specified in these Requirements or the profile specified in Version 1.8.7 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. Effective 2024-03-15, the CA SHALL issue CRLs in accordance with the profile specified in these Requirements.

If the CA asserts compliance with these Baseline Requirements, all CRLs that it issues MUST comply with the following CRL profile, which incorporates, and is derived from RFC 5280. Except as explicitly noted, all normative requirements imposed by RFC 5280 shall apply, in addition to the normative requirements imposed by this document. CAs SHOULD examine RFC 5280, Appendix B for further issues to be aware of.

DRAFT

A full and complete CRL is a CRL whose scope includes all Certificates issued by the CA.

A partitioned CRL (sometimes referred to as a "sharded CRL") is a CRL with a constrained scope, such as all Certificates issued by the CA during a certain period of time ("temporal sharding"). Aside from the presence of the Issuing Distribution Point extension (OID 2.5.29.28) in partitioned CRLs, both CRL formats are syntactically the same from the perspective of this profile.

Minimally, CAs MUST issue either a "full and complete" CRL or a set of "partitioned" CRLs which cover the complete set of Certificates issued by the CA within 7 days of such CA issuing its first certificate. In other words, if issuing only partitioned CRLs, the combined scope of those CRLs must be equivalent to that of a full and complete CRL.

CAs MUST NOT issue indirect CRLs (i.e., the issuer of the CRL is not the issuer of all Certificates that are included in the scope of the CRL).

CRL Fields

Field	**Presence**	**Description**
`tbsCertList`		
`version`	MUST	MUST be v2(1), see Section 7.2.1
`signature`	MUST	See Section 7.1.3.2
`issuer`	MUST	MUST be byte-for-byte identical to the `subject` field of the Issuing CA.
`thisUpdate`	MUST	Indicates the issue date of the CRL.
`nextUpdate`	MUST	Indicates the date by which the next CRL will be issued. For CRLs covering Subscriber Certificates, at most 10 days after the `thisUpdate`. For other CRLs, at most 12 months after the `thisUpdate`.
`revokedCertificates`	*	MUST be present if the CA has issued a Certificate that has been revoked and the corresponding entry has yet to appear on at least one regularly scheduled CRL beyond the revoked Certificate's validity period. The CA SHOULD remove an entry for a corresponding Certificate after it has appeared on at least one regularly scheduled CRL beyond the revoked Certificate's validity period. See the "revokedCertificates Component" table for additional requirements.
`extensions`	MUST	See the "CRL Extensions" table for additional requirements.

Field	Presence	Description
`signatureAlgorithm`	MUST	Encoded value MUST be byte-for-byte identical to the `tbsCertList.signature`.
`signature`	MUST	-
Any other value	NOT RECOMMENDED	-

7.2.1 Version number(s)

Certificate Revocation Lists MUST be of type X.509 v2.

7.2.2 CRL and CRL entry extensions

CRL Extensions

Extension	Presence	Critical	Description
`authorityKeyIdentifier`	MUST	N	See Section 7.1.2.11.1
`CRLNumber`	MUST	N	MUST contain an INTEGER greater than or equal to zero (0) and less than 2^{159}, and convey a strictly increasing sequence.
`IssuingDistributionPoint`	*	Y	See Section 7.2.2.1 CRL Issuing Distribution Point
Any other extension	NOT RECOMMENDED	-	-

revokedCertificates Component

Component	Presence	Description
`serialNumber`	MUST	MUST be byte-for-byte identical to the `serialNumber` contained in the revoked Certificate.
`revocationDate`	MUST	Normally, the date and time revocation occurred. See the footnote following this table for circumstances where backdating is permitted.
`crlEntryExtensions`	*	See the “crlEntryExtensions Component” table for additional requirements.

DRAFT

Note: The CA 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. 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 implementations that process the revocationDate field as the date when the Certificate is first considered to be compromised.

crlEntryExtensions Component

CRL Entry Extension	Presence	Description
`reasonCode`	*	When present (OID 2.5.29.21), MUST NOT be marked critical and MUST indicate the most appropriate reason for revocation of the Certificate.MUST be present unless the CRL entry is for a Certificate not technically capable of causing issuance and either 1) the CRL entry is for a Subscriber Certificate subject to these Requirements revoked prior to 2023-07-15 or 2) the reason for revocation (i.e., reasonCode) is unspecified (0).See the "CRLReasons" table for additional requirements.
Any other value	NOT RECOMMENDED	-

CRLReasons

RFC 5280 reasonCode	RFC 5280 reasonCode value	Description
unspecified	0	Represented by the omission of a reasonCode. MUST be omitted if the CRL entry is for a Certificate not technically capable of causing issuance unless the CRL entry is for a Subscriber Certificate subject to these Requirements revoked prior to 2023-07-15.
keyCompromise	1	Indicates that it is known or suspected that the Subscriber's Private Key has been compromised.
affiliationChanged	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.

DRAFT

RFC 5280 reasonCode	RFC 5280 reason Code value	Description
superseded	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	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.
certificateHold	6	MUST NOT be included if the CRL entry is for 1) a Certificate subject to these Requirements, or 2) a Certificate not subject to these Requirements and was either A) issued on-or-after 2020-09-30 or B) has a `notBefore` on-or-after 2020-09-30.
privilegeWithdrawn	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 about the revocation reason options listed above and provide explanation about when to choose each option. Tools that the CA provides to the Subscriber MUST allow for these options to be easily specified when the Subscriber requests revocation of their 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 the CA and not the Subscriber.

When a CA 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, the CA SHOULD update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension.

7.2.2.1 CRL Issuing Distribution Point

Partitioned CRLs MUST contain an Issuing Distribution Point extension. The `distributionPoint` field of the Issuing Distribution Point extension MUST be present. Additionally, the `fullName` field of the `DistributionPointName` value MUST be present, and its value MUST conform to the following requirements:

1. If a Certificate within the scope of the CRL contains a CRL Distribution Points extension, then at least one of the `uniformResourceIdentifiers` in the CRL Distribution Points's `fullName` field MUST be included in the `fullName` field of the CRL's Issuing Distribution Point extension. The encoding of the `uniformResourceIdentifier` value in the Issuing Distribution Point extension SHALL be byte-for-byte identical to the encoding used in the Certificate's CRL Distribution Points extension.
2. Other GeneralNames of type `uniformResourceIdentifier` MAY be included.
3. Non-`uniformResourceIdentifier` GeneralName types MUST NOT be included.

The `indirectCRL` and `onlyContainsAttributeCerts` fields MUST be set to FALSE (i.e., not asserted).

The CA MAY set either of the `onlyContainsUserCerts` and `onlyContainsCACerts` fields to TRUE, depending on the scope of the CRL.

The CA MUST NOT assert both of the `onlyContainsUserCerts` and `onlyContainsCACerts` fields.

The `onlySomeReasons` field SHOULD NOT be included; if included, then the CA MUST provide another CRL whose scope encompasses all revocations regardless of reason code.

This extension is NOT RECOMMENDED for full and complete CRLs.

7.3 OCSP profile

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross-Certified Subordinate CA 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 Section 7.2.2.

DRAFT

7.3.1 Version number(s)

7.3.2 OCSP extensions

The `singleExtensions` of an OCSP response MUST NOT contain the `reasonCode` (OID 2.5.29.21) CRL entry extension.

DRAFT

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CA SHALL at all times:

1. Comply with these Requirements;
2. Comply with the audit requirements set forth in this section; and
3. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

8.1 Frequency or circumstances of assessment

Certificates that are capable of being used to issue new certificates MUST either be Technically Constrained in line with Section 7.1.2.3, Section 7.1.2.4, or Section 7.1.2.5, as well as audited in line with Section 8.7 only, or Unconstrained and fully audited in line with all remaining requirements from this section. A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 `basicConstraints` extension, with the `cA` boolean set to TRUE and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.4, then no pre-issuance readiness assessment is necessary.

8.2 Identity/qualifications of assessor

The CA's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an eligible audit scheme (see Section 8.4);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

DRAFT

8.3 Assessor's relationship to assessed entity

8.4 Topics covered by assessment

The CA SHALL undergo an audit in accordance with one of the following schemes:

1. WebTrust:
    - "Principles and Criteria for Certification Authorities" Version 2.2 or newer; and either
        - "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security" Version 2.7 or newer; or
        - "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline" Version 2.8 or newer and "WebTrust Principles and Criteria for Certification Authorities – Network Security" Version 1.0 or newer
2. ETSI:
    - ETSI EN 319 411-1 v1.4.1 or newer, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied); or
3. Other:
    - If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either
        a. encompasses all requirements of one of the above schemes; or
        b. consists of comparable criteria that are available for public review.

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 Section 8.2.

For Delegated Third Parties which are not Enterprise RAs, then the CA SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in Section 8.4, that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's Certificate Policy and/or Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then the CA SHALL not allow the Delegated Third Party to continue performing delegated functions.

The audit period for the Delegated Third Party SHALL NOT exceed one year (ideally aligned with the CA's audit).

DRAFT

8.5 Actions taken as a result of deficiency

8.6 Communication of results

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1. The CA SHALL make the Audit Report publicly available.

The CA MUST make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, the CA SHALL provide an explanatory letter signed by the Qualified Auditor.

The Audit Report MUST contain at least the following clearly-labelled information:

1. name of the organization being audited;
2. name and address of the organization performing the audit;
3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross-Certified Subordinate CA Certificates, that were in-scope of the audit;
4. audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
5. a list of the CA policy documents, with version numbers, referenced during the audit;
6. whether the audit assessed a period of time or a point in time;
7. the start date and end date of the Audit Period, for those that cover a period of time;
8. the point in time date, for those that are for a point in time;
9. the date the report was issued, which will necessarily be after the end date or point in time date; and
10. (for audits conducted in accordance with any of the ETSI standards) a statement to indicate if the audit was a full audit or a surveillance audit, and which portions of the criteria were applied and evaluated, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part 1 (General Requirements), and/or Part 2 (Requirements for Trust Service Providers).
11. (for audits conducted in accordance with any of the ETSI standards) a statement to indicate that the auditor referenced the applicable CA/Browser Forum criteria, such as this document, and the version used.

An authoritative English language version of the publicly available audit information MUST be provided by the Qualified Auditor and the CA SHALL ensure it is publicly available.

The Audit Report MUST be available as a PDF, and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report MUST be uppercase letters and MUST NOT contain colons, spaces, or line feeds.

DRAFT

8.7 Self-Audits

During the period in which the CA issues Certificates, the CA SHALL monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Effective 2025-03-15, the CA 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.

Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 8.4, the CA SHALL strictly control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. The CA SHALL review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.

The CA SHALL internally audit each Delegated Third Party's compliance with these Requirements on an annual basis.

During the period in which a Technically Constrained Subordinate CA issues Certificates, the CA which signed the Subordinate CA SHALL monitor adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practice Statement. On at least a quarterly basis, against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by the Subordinate CA, during the period commencing immediately after the previous audit sample was taken, the CA shall ensure all applicable CP are met.

DRAFT

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

9.1.2 Certificate access fees

9.1.3 Revocation or status information access fees

9.1.4 Fees for other services

9.1.5 Refund policy

9.2 Financial responsibility

9.2.1 Insurance coverage

9.2.2 Other assets

9.2.3 Insurance or warranty coverage for end-entities

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

9.3.2 Information not within the scope of confidential information

9.3.3 Responsibility to protect confidential information

9.4 Privacy of personal information

9.4.1 Privacy plan

9.4.2 Information treated as private

9.4.3 Information not deemed private

9.4.4 Responsibility to protect private information

9.4.5 Notice and consent to use private information

9.4.6 Disclosure pursuant to judicial or administrative process

9.4.7 Other information disclosure circumstances

DRAFT

9.5 Intellectual property rights

9.6 Representations and warranties

9.6.1 CA representations and warranties

By issuing a Certificate, the CA 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.

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

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, the CA
    i. 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);
    ii. followed the procedure when issuing the Certificate; and
    iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
2. **Authorization for Certificate**: That, at the time of issuance, the CA
    i. 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;
    ii. followed the procedure when issuing the Certificate; and
    iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
3. **Accuracy of Information**: That, at the time of issuance, the CA
    i. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate;
    ii. followed the procedure when issuing the Certificate; and

DRAFT

iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

4. **Identity of Applicant**: That, if the Certificate contains Subject Identity Information, the CA
    i. implemented a procedure to verify the identity of the Applicant in accordance with Section 3.2 and Section 7.1.2;
    ii. followed the procedure when issuing the Certificate; and
    iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
5. **Subscriber Agreement**: That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
6. **Status**: That the CA 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 the CA will revoke the Certificate for any of the reasons specified in these Requirements.

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

The CA SHALL require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's acknowledgement of the Terms of Use.

The CA SHALL implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate

request. The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information**: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures to assure 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);
3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate**: An obligation and warranty to install the Certificate only on servers that are accessible at the `subjectAltName`(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
5. **Reporting and Revocation**: 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, and
    b. promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance**: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to

DRAFT

violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the CA's CP, CPS, or these Baseline Requirements.

9.6.4 Relying party representations and warranties

9.6.5 Representations and warranties of other participants

9.7 Disclaimers of warranties

9.8 Limitations of liability

For delegated tasks, the CA and any Delegated Third Party MAY allocate liability between themselves contractually as they determine, but the CA SHALL remain fully responsible for the performance of all parties in accordance with these Requirements, as if the tasks had not been delegated.

If the CA has issued and managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA 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 the CA's Certificate Policy and/or Certification Practice Statement.

If the CA has not issued or managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA 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 the CA desires.

If the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement, then the CA SHALL include the limitations on liability in the CA's Certificate Policy and/or Certification Practice Statement.

9.9 Indemnities

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA 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 the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, the CA 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 the CA, 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 the CA 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 the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and termination

9.10.1 Term

9.10.2 Termination

9.10.3 Effect of termination and survival

9.11 Individual notices and communications with participants

9.12 Amendments

9.12.1 Procedure for amendment

9.12.2 Notification mechanism and period

9.12.3 Circumstances under which OID must be changed

9.13 Dispute resolution provisions

9.14 Governing law

9.15 Compliance with applicable law

The CA SHALL issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates.

DRAFT

9.16 Miscellaneous provisions

9.16.1 Entire agreement

9.16.2 Assignment

9.16.3 Severability

In the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which a CA operates or issues certificates, a CA 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, the CA SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of the CA's CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by the CA.

The CA MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

Any modification to CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to the CA's CPS and a notice to the CA/Browser Forum, as outlined above, MUST be made within 90 days.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

9.16.5 Force Majeure

9.17 Other provisions

DRAFT

Appendix A – CAA Contact Tag

These methods allow domain owners to publish contact information in DNS for the purpose of validating domain control.

A.1. CAA Methods

A.1.1. CAA contactemail Property

SYNTAX: `contactemail <rfc6532emailaddress>`

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 following is an example where the holder of the domain specified the contact property using an email address.

```
$ORIGIN example.com .
CAA 0 contactemail "domainowner@example.com"
```

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.

A.1.2. CAA contactphone Property

SYNTAX: `contactphone <rfc3966 Global Number>`

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 spaces as visual separators.

The following is an example where the holder of the domain specified the contact property using a phone number.

```
$ORIGIN example.com .
CAA 0 contactphone "+1 555 123 4567"
```

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.

A.2. DNS TXT Methods

A.2.1. DNS TXT Record Email Contact

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

DRAFT

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.

A.2.2. DNS TXT Record Phone Contact

The 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.

DRAFT

Appendix B – Issuance of Certificates for Onion Domain Names

This appendix defines permissible verification procedures for including one or more Onion Domain Names in a Certificate.

1. The ADN MUST contain at least two Domain Labels, where the rightmost Domain Label is "onion", and the Domain Label immediately preceding the rightmost "onion" Domain Label is a valid Version 3 Onion Address, as defined in Section 6 of the Tor Rendezvous Specification - Version 3 located at https://spec.torproject.org/rend-spec-v3.
2. The CA MUST verify the Applicant's control over the ADN using at least one of the methods listed below:
    a. The CA MAY verify the Applicant's control over the ADN by using any method from Section 3.2.2.4 that says "This method allows Onion Domain Name issuance", with this modification:

       When these methods are used to verify the Applicant's control over an Onion Domain Name, the CA MUST use Tor protocol to establish a connection to the ADN. The CA MUST NOT delegate or rely on a third-party to establish the connection, such as by using Tor2Web.

       Note: This section does not override or supersede any provisions specified within the respective methods. The CA MUST only use a method if it is still permitted within that section.

    b. The CA MAY verify the Applicant's control over the .onion service corresponding to the ADN by having the Applicant provide a Certificate Request signed using the .onion service's private key if the Attributes section of the certificationRequestInfo contains:

       i. A caSigningNonce attribute that contains a Random Value that is generated by the CA; and
       ii. An applicantSigningNonce attribute that contains a single value. The CA MUST recommend to Applicants that the applicantSigningNonce value should contain at least 64 bits of entropy.

       The signing nonce attributes have the following format:

```
cabf OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
international-organizations(23) ca-browser-forum(140) }

caSigningNonce ATTRIBUTE ::= {
   WITH SYNTAX               OCTET STRING
   EQUALITY MATCHING RULE    octetStringMatch
   SINGLE VALUE              TRUE
   ID                        { cabf-caSigningNonce }
}
```

DRAFT

```
cabf-caSigningNonce OBJECT IDENTIFIER ::= { cabf 41 }

applicantSigningNonce ATTRIBUTE ::= {
   WITH SYNTAX               OCTET STRING
   EQUALITY MATCHING RULE    octetStringMatch
   SINGLE VALUE              TRUE
   ID                        { cabf-applicantSigningNonce }
}

cabf-applicantSigningNonce OBJECT IDENTIFIER ::= { cabf 42 }
```

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.

3. When a Certificate includes an Onion Domain Name, the Domain Name shall not be considered an Internal Name provided that the Certificate was issued in compliance with this Appendix B.

DRAFT