Apple Inc.

Apple Public Root Certificate Policy

Version 2.0

Effective Date: September 1, 2023

Table of Contents

1. INTRODUCTION

1.1. OVERVIEW

This Certificate Policy (CP) describes the requirements employed by Apple Inc. acting as a publicly-trusted Root Certification Authority ("Apple Public CA") in issuing and managing digital Certificates and related services to:

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

This CP describes an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements that are necessary for the issuance and management of Publicly-Trusted Certificates; Certificates that are trusted by virtue of the fact that their corresponding Root Certificate is distributed in widely-available application software.

The Apple Public CA develops, implements, enforces, and annually updates a CP and a Certification Practice Statement (CPS) that describe in detail how the Apple Public CA implements the latest version of the Requirements.

This CP conforms to the current versions of the following policies, guidelines, and requirements:

Name of Policy/ Guideline/ Requirement Standard	Location of Source Document
The Certification Authority / Browser Forum ("CA/ Browser Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")	https://cabforum.org/baseline-requirements-documents/
The CA/Browser Forum Network and Certificate System Security Requirements	https://cabforum.org/network-security-requirements/
Apple Root Store Program	https://www.apple.com/certificateauthority/ca_program.html
Chromium Root Store Policy	https://www.chromium.org/Home/chromium-security/root-ca-policy
Microsoft Root Certificate Program	https://docs.microsoft.com/en-us/security/trusted-root/program-requirements
Mozilla Root Store Policy	https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
Oracle Java Root Certificate Program	https://www.oracle.com/technetwork/java/javase/javasecarootcertsprogram-1876540.html

The Apple Public CA requires that Subscriber Certificates include at least one policy object identifier (OID) as a way to assert that the Apple Public CA makes commercially reasonable efforts to conform to the latest version of the CA/Browser Forum Baseline Requirements and the Application Software Suppliers programs described in the table above.

In the event of inconsistency between governing requirements, requirements of the Application Software Supplier programs take precedence over the Baseline Requirements, which take precedence over this CP, which takes precedence over specifications articulated in the Issuing CA's CPS.

This CP is structured according to RFC 3647 and includes at least every section and subsection defined in RFC 3647. There are sections that include the words "No Stipulation", which mean that no particular requirements are imposed in relation to that section. This CP contains no sections that are blank.

1.2. DOCUMENT NAME AND IDENTIFICATION

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

{iso(1) member-body(2)
us(840)
apple(113635)
appleDataSecurity(100)
appleCertificatePolicies(5)
applePublicPolicyID(19)}
(1.2.840.113635.100.5.19)

CP and CPS documents SHALL be assigned different OIDs under separate branches.

This is the Apple Public Root Certificate Policy ("Apple Public Root CP"). The name reflects the publicly-trusted nature of the Certification Authorities regulated by it and is assigned this OID:

aprCProot ::= {applePublicPolicyID (1) aprCP (1) 1} — (1.2.840.113635.100.5.19.1.1.1)

1.2.1. Revisions

This CP is reviewed and updated at least annually, as required by the Baseline Requirements. This is the list of revisions:

Date	Changes	Version
09/1/2023	Updated multiple sections to bring the document to compliance with Baseline Requirements up to version 2.0. and S/MIME Baseline Requirements up to version 1.0.1.	2.0

Date	Changes	Version
11/15/2022	Included Section 1.2.2 to mirror CA/Browser Forum Baseline Requirements related to pending relevant dates. Updated Section 2.2 to incorporate requirements about posting CP/CPS documents in Repository and CCADB. Updated Section 5.7.1 to add cross-references to Mozilla and Microsoft incident response requirements.	1.3
10/01/2022	Updated Sections 2.2, 4.9.1.1, 4.9.3, 4.9.9, 6.1.1.3, 7.2.2, 9.6.1 for compliance with Mozilla Root Store Policy version 2.8. Updated Section 4.9.9 for compliance with Apple Root Certificate Program. Made minor editorial changes to Sections 1.2.1, 1.3.2 and 4.4.3	1.2
09/01/2022	Updated Sections 3.2.2.4, 3.2.2.8, 4.1.1, 5.4.1, 5.4.2, 5.4.3, 5.4.6, 5.5.1, 5.5.2, Appendix B and Appendix C for compliance with CABF Baseline Requirements from versions 1.8.1 up to 1.8.4.	1.1
12/09/2021	Initial release.	1.0

1.2.2. Relevant Dates

Some requirements have a compliance date in the future in relationship to the publication of specific version. Those requirements are listed below with the expected compliance date and a brief description.

Compliance Date	Section	Summary Description
06/11/2022	7.1.3.2.1	CAs MUST NOT sign OCSP responses using the SHA-1 hash algorithm. Note: This requirement was implemented in version 1.0 of this CP.
09/01/2022	7.1.4.2.2	CAs MUST NOT include the organizationalUnitName field in the Subject. Note: This requirement was implemented in version 1.0 of this CP.

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

A Certification Authority (CA) is 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.

1.3.2. Registration Authorities

A Registration Authority (RA) is 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.

With the exception of Section 3.2.2.4 and Section 3.2.2.5, 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 the requirements in this CP that are applicable to the delegated function, and
4. Comply with
    a. the Issuing CA's CPS or
    b. the Delegated Third Party's practice statement that the CA has verified complies with this CP.

1.3.2.2. Enterprise registration authorities

For TLS Certificates:

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.

For S/MIME Certificates:

The CA MAY delegate to an Enterprise Registration Authority (RA) to verify Certificate Requests for Subjects within 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. If the Certificate Request is for a `Mailbox-validated`, `Organization-validated`, or `Sponsor-validated` profile, the CA SHALL confirm that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with Section 3.2.4.1 or Section 3.2.5.3.
2. The CA SHALL confirm that the `subject:organizationName` name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, 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 as defined in Section 3.2 or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested email domain falls within the subdomains of ABC Co.'s Registered Domain Name.

The CA SHALL impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA in accordance with Section 8.8.

An Enterprise RA MAY also submit Certificate Requests using the Mailbox-validated profile for users whose email domain(s) are not under the delegated organization's authorization or control. In this case, the CA SHALL confirm that the mailbox holder has control of the requested Mailbox Address(es) in accordance with Section 3.2.4.2.

1.3.3. Subscribers

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.

1.3.4. Relying Parties

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.

1.3.5. Other Participants

1.3.5.1. CA/Browser Forum

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

1.3.5.2. Application Software Supplier

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

1.3.5.3. Apple Policy Authority

The Apple Policy Authority (APA) is a multi-disciplinary group from within Apple Inc. responsible for interpretation of the Requirements, maintenance, and approval of this CP and approval of Issuing CA's CPS.

1.4. CERTIFICATE USAGE

For TLS Certificates:

The primary goal of the requirements in this CP is to enable efficient and secure electronic communication, while addressing user concerns about the trustworthiness of Certificates. This CP also serves to inform users and help them to make informed decisions when relying on Certificates.

For S/MIME Certificates:

The primary goal of the requirements in this CP is to provide a framework of "reasonable assurance" to senders and recipients of email messages that the Subject identified in an S/MIME Certificate has control of the domain or Mailbox Address being asserted. A variation of this use case is where an Individual or organization digitally signs email to establish its authenticity and source of origin.

These Requirements describe an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements for the issuance and management of Publicly-Trusted S/MIME Certificates. These Requirements also serve to inform users and help them to make informed decisions when relying on Certificates.

1.4.1. Appropriate Certificate Uses

A Certificate's use SHALL be conveyed to Relying Parties through values in the keyUsage and extendedKeyUsage extensions. This CP provides further requirements in Section 7.1.2.1, 7.1.2.2 and 7.1.2.3.

This CP sanctions the following uses:

For CA Certificates:

Signature of other Certificates, CRLs and OCSP responses

For TLS Certificates:

Server Authentication and Client Authentication

For S/MIME Certificates:

Secure Email and Client Authentication

1.4.2. Prohibited Certificate Uses

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

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

This CP is administered by the APA.

1.5.2. Contact Person

The contact information for this CP is:

Apple Policy Authority
One Apple Park Way
Cupertino, CA 95014

(408) 996-1010
policy_authority@apple.com

1.5.2.1. Certificate Problem Reporting

To submit a Certificate Problem Report, PKI Participants and other third parties SHALL use: contact_pki@apple.com.

1.5.3. Person Determining CPS Suitability for the Policy

The APA determines the suitability and applicability of this CP.

The APA SHALL determine the compliance of an Issuing CA's CPS to this CP.

1.5.4. CPS Approval Procedures

The APA approves all amendments to this CP and Issuing CAs' Certification Practices Statements.

Document amendments MUST be evidenced by a new version number and date recorded in Section 1.2.1., except when the amendments are purely clerical.

Documents SHALL become effective and superseded based on Section 9.10.1 and Section 9.10.2.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

See Appendix C.

1.6.2. Acronyms

See Appendix C.

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 319 403-1, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1 - 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

ETSI EN 319 411-2, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

ETSI EN 319 412-1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

ETSI EN 319 412-5, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

ETSI TS 119 172-4, Electronic Signatures and Infrastructures (ESI); Signature Policies;. Part 4: Signature applicability rules.

ETSI TS 119 495, Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking.

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

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

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

ICAO DOC 9303, Machine Readable Travel Documents, Part 10, Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC), International Civil Aviation Organization, Eighth Edition, 2021.

ICAO DOC 9303, Machine Readable Travel Documents, Part 11, Security Mechanisms for MRTDs, International Civil Aviation Organization, Eighth Edition, 2021.

ISO 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services.

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

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

ISO 21188:2006, Public key infrastructure for financial services – Practices and policy framework.

Network and Certificate System Security Requirements, Version 1.7, available at https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Network-Security-Guidelines-v1.7.pdf.

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

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

RFC3492, Request for Comments: 3492, Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA). A. Costello. March 2003.

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

RFC3739, Request for Comments: 3739, Internet X.509 Public Key Infrastructure: Qualified Certificates Profile, S. Santesson, et al. March 2004.

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

RFC3986, Request for Comments: 3986, Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee, et al. January 2005.

RFC4262, Request for Comments: 4262, X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities, S. Santesson. December 2005.

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments. A. Deacon, et al. September 2007.

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

RFC5890, Request for Comments: 5890, Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework. J. Klensin. August 2010.

RFC5952, Request for Comments: 5952, A Recommendation for IPv6 Address Text Representation. S. Kawamura, et al. August 2010.

RFC6818, Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. January 2013.

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

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

RFC7231, Request For Comments: 7231, Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. R. Fielding, et al. June 2014.

RFC7482, Request for Comments: 7482, Registration Data Access Protocol (RDAP) Query Format, A. Newton, et al. March 2015.

RFC7538, Request For Comments: 7538, The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect), J. Reschke. April 2015.

RFC8499, Request for Comments: 8499, DNS Terminology. P. Hoffman, et al. January 2019.

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

WebTrust for Certification Authorities, CPA Canada.

WebTrust for Certification Authorities, SSL Baseline with Network Security, Version 2.5, https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/wt100bwtbr-25-110120-finalaoda.pdf.

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.

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

"TLS Baseline Requirements" means the relevant version of the CA/Browser Forum's "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates". See https://cabforum.org/baseline-requirements-documents/.

1.6.4. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this CP shall be interpreted in accordance with RFC 2119.

By convention, this CP 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.

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 CP.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

The Apple Public CA publishes the current and older versions of this CP on https://www.apple.com/certificateauthority/public/, which is available on a 24x7 basis. Updated versions of this CP are uploaded to the CCADB within seven days of APA approval.

The Issuing CA SHALL publicly disclose current and older versions of its CPS through an appropriate and readily accessible online means that is available on a 24x7 basis. The Issuing CA SHALL upload an updated version of its CPS to the CCADB within seven days of APA approval. 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 Issuing CA's CPS MUST be structured in accordance with RFC 3647 and MUST include all material required by RFC 3647.

For TLS Certificates:

Section 4.2 of an Issuing CA's CPS SHALL state the CA's practice on processing CAA Records for Fully-Qualified Domain Names, which SHALL be consistent with the requirements in this CP. It SHALL clearly specify the set of Issuer Domain Names that the CA recognizes in CAA "issue" or "issuewild" records as permitting it to issue. The CA SHALL log all actions taken, if any, consistent with its processing practice.

The CA SHALL publicly give effect to the requirements in this CP and represent that it will adhere to the latest published version. The CA MAY fulfill this requirement by incorporating the Requirements directly into its CP 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 Certificates published at http://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.

For S/MIME Certificates:

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 CP and/or CPS or by incorporating them by reference using a clause such as the following (which SHALL 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 S/MIME 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.*

2.3. TIME OR FREQUENCY OF PUBLICATION

The CA SHALL develop, implement, enforce, and annually update a CP and/or CPS that describes in detail how the CA implements the latest version of the 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.

The Apple Public CA develops, implements, enforces, and annually updates this CP that describes the latest version of the relevant requirements set forth in Section 1.1.

CAs SHALL develop, implement, enforce, and annually update a CPS that describes in detail how the CA implements practices that meet the requirements in this CP. The CA SHALL indicate conformance with this requirement by incrementing the version number and adding a dated log 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.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

For TLS Certificates:

No stipulation.

For S/MIME Certificates:

When the `subject:commonName` of a Certificate issued to an Individual does not contain a Mailbox Address, it is specified as a Personal Name or Pseudonym as described in Section 7.1.4.2.2.

Names consisting of multiple words are permitted. Given names joined with a hyphen are considered as one single given name. Subjects with more than one given name MAY choose one or several of their given names in any sequence. Subjects MAY choose the order of their given name(s) and surname in accordance with national preference.

The CA MAY allow common variations or abbreviations of Personal Names consistent with local practice.

3.1.2. Need for Names To Be Meaningful

For TLS Certificates:

No stipulation.

For S/MIME Certificates:

Personal Names SHALL be a meaningful representation of the Subject's name as verified in the identifying documentation or Enterprise RA records.

3.1.3. Anonymity Or Pseudonymity Of Subscribers

For TLS Certificates:

No stipulation.

For S/MIME Certificates:

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

For `Sponsor-validated` certificates, the CA MAY use a `subject:pseudonym` attribute in the Certificate if the associated Subject has been verified according to Section 3.2.3. If present, the subject:pseudonym attribute SHALL be:

1. Either a unique identifier selected by the CA for the Subject of the Certificate, or

2. An identifier selected by the Enterprise RA which uniquely identifies the Subject of the Certificate within the Organization included in the `subject:organizationName` attribute.

For `Individual-validated` certificates, the CA MAY use the `subject:pseudonym` attribute if the associated Subject has been verified according to Section 3.2.3. If present, the subject:pseudonym attribute SHALL be:

1. Either a unique identifier selected by the CA for the Subject of the Certificate, or
2. An identifier verified based on government-issued identity documents.

Pseudonym Certificates are not anonymous. CAs and Enterprise RAs SHALL treat Individual identity information relating to a Pseudonym as private in accordance with Section 9.4.2.

3.1.4. Rules of Interpreting Various Name Forms

For TLS Certificates:

No stipulation.

For S/MIME Certificates:

3.1.4.1. Non ASCII character substitution

The CA MAY allow the Conversion of Subject Identity Information usually rendered in non-ASCII characters (including Accent or Umlaut-accented characters) using a system commonly used in the Applicant's Jurisdiction of Incorporation or Registration, or recognized by the United Nations or the International Organization for Standardization (ISO). The CA SHOULD state the used Conversion systems in its CP and/or CPS. For example, regardless of capitalization:

- Accent characters MAY be represented by their ASCII equivalent. For example é, à, í, ñ, or ç MAY be represented by e, a, i, n, or c, respectively.
- Umlaut-accented characters such as ä, ö, ü MAY be represented by either ae, oe, ue or a, o, u, respectively.

The CA MAY include an ASCII character name that is not a direct Conversion of the Applicant's registered name provided that it is verified in a Reliable Data Source or suitable Attestation.

3.1.4.2. Geographic names

The CA MAY use geographic endonyms and exonyms in the `subject:localityName` and `subject:stateOrProvinceName` attributes, (e.g., Munich, Monaco di Bavaria, or Мюнхен for München). The CA SHOULD avoid the use of archaic geographic names, (e.g., prefer Mumbai over Bombay).

3.1.5. Uniqueness of Names

For TLS Certificates:

Issuing CAs SHALL enforce Subject Distinguished Name uniqueness for Root Certificates.

For S/MIME Certificates:

No stipulation.

3.1.6. Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2. INITIAL IDENTITY VALIDATION

The CA SHALL authenticate the identity attributes of the Subject and their control over the Domains, IP Addresses, and Mailbox Addresses to be included in the Certificate according to the requirements of the following sections:

Certificate Type	Organization Identity	Individual Identity	Domain Control	IP Address Control	Mailbox Control
TLS	Section 3.2.2.1	-	Section 3.2.2.4	Section 3.2.2.5	-
S/MIME: Mailbox-validated	-	-	Section 3.2.4.1, Section 3.2.2.4	-	Section 3.2.4
S/MIME: Organization-validated	Section 3.2.5	-	Section 3.2.4.1, Section 3.2.2.4	-	Section 3.2.4
S/MIME: Sponsor-validated	Section 3.2.5	Section 3.2.3	Section 3.2.4.1, Section 3.2.2.4	-	Section 3.2.4
S/MIME: Individual-validated	-	Section 3.2.3	Section 3.2.4.1, Section 3.2.2.4	-	Section 3.2.4

3.2.1. Method To Prove Possession of Private Key

No stipulation.

3.2.2. Authentication of Organization Identity, Domain Identity and Email Control - TLS Certificates

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 Issuing CA's CPS.

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 Section 3.2.2.1 and that is

described in the CA's CPS. 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,
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.

3.2.2.4. Validation of Domain Authorization or Control

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

The CA SHALL confirm that prior to issuance, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate as follows:

1. When the FQDN is not an Onion Domain Name, the CA SHALL validate the FQDN using at least one of the methods listed below; and
2. When the FQDN is an Onion Domain Name, the CA SHALL validate the FQDN 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.

CAs SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

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

3.2.2.4.1. Validating the Applicant as a Domain Contact

This method has been retired and MUST NOT be used.

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

Confirming the Applicant's control over the FQDN 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 a Domain Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.

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 Domain Name Registrar as representing the Domain Name Registrant for every FQDN 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.

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

3.2.2.4.3. Phone Contact with Domain Contact

This method has been retired and MUST NOT be used.

3.2.2.4.4. Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN 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 an Authorization Domain Name, and
2. including a Random Value in the email, and
3. receiving a confirming response utilizing the Random Value.

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

The Random Value SHALL be unique in each email.

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

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

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

3.2.2.4.5. Domain Authorization Document

This method has been retired and MUST NOT be used.

3.2.2.4.6. Agreed-Upon Change to Website

This method has been retired and MUST NOT be used.

3.2.2.4.7. DNS Change

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a 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).

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

3.2.2.4.8. IP Address

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

Note: Once the FQDN has been validated using this method, the CA MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN

using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.9. Test Certificate

This method has been retired and MUST NOT be used.

3.2.2.4.10. TLS Using a Random Number

This method has been retired and MUST NOT be used.

3.2.2.4.11. Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.4.12. Validating Applicant as a Domain Contact

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

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

3.2.2.4.13. Email to DNS CAA Contact

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

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

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

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

3.2.2.4.14. Email to DNS TXT Contact

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

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

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

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

3.2.2.4.15. Phone Contact with Domain Contact

Confirm the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

In the event that someone other than a Domain Contact is reached, the CA MAY request to be transferred to the Domain Contact.

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 Issuing CA's CPS MAY specify a shorter validity period for Random Values.

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

3.2.2.4.16. Phone Contact with DNS TXT Record Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the ADN. 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 they provide 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 Issuing CA's CPS MAY specify a shorter validity period for Random Values.

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

3.2.2.4.17. Phone Contact with DNS CAA Phone Contact

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

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 Issuing CA's CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the

validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.18. Agreed-Upon Change to Website v2

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

1. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file, and
2. 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 Number:

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

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

Note: The CA MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.19. Agreed-Upon Change to Website - ACME

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

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 Issuing CA's 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.

Note: The CA MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.20. TLS Using ALPN

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] 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 Issuing CA's CPS MAY specify a shorter validity period for the token, in which case the CA MUST follow its CPS.

Note: Once the FQDN has been validated using this method, the CA MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

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.

CAs SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address.

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:

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 this document).

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

3.2.2.5.3. Reverse Address Lookup

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

3.2.2.5.4. Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.5.5. Phone Contact with IP Address Contact

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 Issuing CA's CPS MAY specify a shorter validity period for Random Values.

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 draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

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 draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

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.

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

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. If the CA issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

This stipulation does not prevent the CA from checking 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.

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 the Baseline Requirements, CAs MUST NOT rely on any exceptions specified in their Certificate Practices Statement 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 7.1.2.1, 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 domain's zone does not have a DNSSEC validation chain to the ICANN root.

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:.

3.2.3. Authentication of Individual Identity

For TLS Certificates:

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.

For S/MIME Certificates:

The following requirements SHALL be fulfilled to authenticate Individual identity attributes included in `Sponsor-validated` and `Individual-validated` Certificate profiles.

The CA or RA SHALL collect and retain evidence supporting the following identity attributes for the Individual Applicant:

1. Given name(s) and surname(s), which SHALL be current names,
2. Pseudonym (if used),
3. Title (if used),
4. Address (if displayed in Subject), and
5. Further information as needed to uniquely identify the Applicant.

The CA, RA, or Enterprise RA SHALL comply with applicable data protection legislation in the gathering and retention of evidence relating to Individual identity supporting this Requirement in accordance with Section 9.4.

3.2.3.1. Attribute collection of individual identity

The CA SHALL document and publish the methods it uses to collect Individual identity attributes.

3.2.3.1.1. From a physical identity document

If physical identity documents are used as evidence, the CA or RA SHALL accept only government-issued passports or identity cards, and other official identity documents of comparable reliability (such as drivers license or military ID).

The physical identity document used as evidence SHALL contain a face photo and/or other information that can be compared with the Applicant's physical appearance.

The CA SHALL document and publish information describing the physical or digital identity documents or document types it accepts.

3.2.3.1.2. From a digital identity document

If digital identity documents (such as passports or national ID cards including a chip bearing digitally signed information about the holder) are used as evidence, the CA or RA SHALL only accept eMRTD digital identity documents according to ICAO 9303 part 10.

This method does not include "eID" as described in Regulation (EU) 910/2014.

3.2.3.1.3. Using electronic identification schemes (eID)

If an eID is used as evidence, the CA or RA SHALL only accept "notified" eID schemes according to Article 9 of the eIDAS Regulation and the eID shall conform to eIDAS LoA "Substantial" or "High".

The CA SHALL document and publish information describing the eID and associated eID attributes it accepts.

3.2.3.1.4. From a certificate supporting a digital signature applied by the Applicant

If a digital signature is to be used as evidence, the CA or RA SHALL have the Applicant digitally sign the Certificate Request using a valid personal Certificate that was issued under an Approved Framework described in this section.

Identity attributes are evidenced by the signing Certificate, not by the content of the signed document. The CA or RA SHALL only rely upon the signing Certificate as evidence for identity attributes if the digital signature is valid in accordance with the requirements of the relevant Approved Framework.

The CA SHOULD consider requirements to avoid issuance of consecutive Certificates that are issued based on a preceding Certificate, where the original verification of the Subject's identity may have been conducted in the distant past.

The CA/Browser Forum S/MIME Certificate Working Group may consider additional trust service frameworks that provide an equivalent level of security and validation compared to these Requirements. Proposals that evaluate the additional framework against the following criteria MAY be submitted to the questions@cabforum.org mailing list:

- Legal context: the framework SHALL be subject to regulatory provisions, which describe the requirements imposed on the Certificate issuer/trust service provider, the legal effects of the trust services, and the corresponding Certificate levels,

- Identity validation: the approved Certificate levels must provide a level of assurance equivalent to that of the identity validation methods described in these Requirements,
- Supervision and auditing systems: the framework SHALL include appropriate rules providing for:
  - supervision to ensure that trust service providers meet regulatory-imposed provisions,
  - requirements imposed on auditing bodies when conducting audits, and
  - supervision of the auditing bodies.
- Best practices and transparency: the requirements of the trust service framework and evidence of supervision of the approved trust service providers SHALL be publicly available. The trust service framework shall require trust service providers to disclose their practices in a publicly available CP and/or CPS.

3.2.3.1.5. From Enterprise RA records

In the case of `Sponsor-validated` Certificates approved by an Enterprise RA, records maintained by the Enterprise RA SHALL be accepted as evidence of Individual identity.

The Enterprise RA SHALL maintain records to satisfy the requirements of Section 1.3.2 and Section 8.8.

3.2.3.1.6. Affiliation from company attestation

In the case of `Sponsor-validated` Certificates not approved by an Enterprise RA, the CA or RA MAY verify the authority or affiliation of an Individual to represent an Organization to be included in the `subject:organizationName` of the Certificate using an Attestation provided by the Organization and verified in accordance with Section 3.2.9.

The CA or RA SHALL still verify the identity of the Individual in accordance with Section 3.2.3 and the Organization in accordance with Section 3.2.5.

3.2.3.1.7. From a general attestation

Evidence for Individual identity attributes MAY be gathered using an Attestation from a qualified legal practitioner or notary in the Applicant's jurisdiction.

3.2.3.1.8. From authorized reference sources as supplementary evidence

Evidence for Individual identity attributes SHALL use at least one of the following sources for authoritative evidence: a physical or digital identity document, digital signature supported by certificate, Enterprise RA records, or suitable Attestation.

The CA or RA MAY additionally gather and verify supplementary evidence using authorized sources such as additional official documents, government or regulatory registers, or national population registers.

Examples of this method include:

- If the Subject presents an ID featuring an Applicant name that has subsequently been changed, the evidence MAY be complemented by inspection of an official document such as a marriage certificate or court order documenting the change.
- If a professional Title of a regulated profession in the `subject:country`, or a corporate Title linked to the `subject:organizationName`, is to be used it SHALL be verified against supporting documentation, a Reliable Data Source, or Attestation.
- In cases where the "role" LEI is included in an extension of a `Sponsor-validated` Certificate, the CA SHALL verify that the LEI is assigned to the Individual and the `subject:organizationName` in the Certificate Subject.
- The CA MAY verify the address (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.

The CA SHALL internally document the accepted reference sources, including a description of the documents or Attestations accepted as supplementary evidence.

3.2.3.2. Validation of individual identity

The CA or RA SHALL validate all identity attributes of the Individual to be included in the Certificate.

If the evidence has an explicit validity period, the CA SHALL verify that the time of the identity validation is within this validity period. In context this can include the `notBefore` and `notAfter` fields of a digital signature Certificate or the date of expiry of an identity document.

The CA or RA MAY reuse existing evidence to validate Individual identity subject to the age restrictions in Section 4.2.1.

3.2.3.2.1. Validation of a physical identity document

The physical identity document SHALL be presented in its original form. The CA SHALL employ procedures to ensure the evidence presented by the Applicant is a genuine identity document that is not counterfeited or falsified/modified.

The CA or RA MAY use manual (in person) or remote procedures. A remote process SHALL ensure that the Applicant has the document in hand and presents the document in real-time in front of a camera.

The CA or RA registration agent SHALL make a visual comparison of the physical appearance of the Applicant and the face photo and/or other information on the physical identity document.

The CA or RA registration agent SHALL have access to authoritative sources of information on document appearance and validation for forms of identity document accepted by the CA.

The CA or RA SHALL retain information sufficient to evidence the fulfillment of the identity validation process and the verified attributes. In addition to identity attributes, the CA or RA SHALL record the following information: issuer, validity period, and the document's unique identification number.

Automated and manual processes MAY be used in combination, (for example the CA or RA may deploy automated tools to support the work of a registration agent, or an automated process that falls back to a registration agent if the process yields an uncertain result).

3.2.3.2.2. Validation of a digital identity document

The CA or RA SHALL only accept digital identity documents if the issuer's digital signature on the document is successfully validated according to ICAO 9303 part 11.

The CA or RA SHALL record information obtained from the digital identity document to evidence the identity proofing process. In addition to identity attributes and face photo, the following information SHALL be recorded: issuer, validity period, and the document's unique identification number.

The CA or RA registration agent SHALL make a visual comparison of the physical appearance of the Applicant and the face photo and/or other information on the digital identity document.

Automated and manual processes MAY be used in combination, (for example using automated tools to support the work of a registration agent, or an automated process that falls back to a registration agent if the process yields an uncertain result).

3.2.3.2.3. Validation of eID

If authentication using an eID is used as evidence, the CA or RA SHALL confirm that the eID scheme is suitable (i.e., that the eID is accessible via a "notified" eIDAS-Node), and that the individual eID is valid (i.e., not expired, suspended, or revoked).

The authentication using the eID SHALL be created as part of the identity validation process, and evidence of the validation with the eID's Identity Provider (IdP) SHALL be retained by the CA or RA.

3.2.3.2.4. Validation of digital signature with certificate

If a digital signature with Certificate is used as evidence, the signature SHALL be created as part of the identity validation process.

The CA or RA SHALL validate the digital signature and SHALL only use the signing Certificate as evidence for identity attributes if the signature is valid.

If required identity attributes to be collected are not present in the Certificate, the CA or RA SHALL collect these attributes from other sources and validate them accordingly.

3.2.3.2.5. Validation of an Attestation

If an Attestation is used as evidence for the validation of Individual identity attributes, then the reliability of the Attestation SHALL be verified according to Section 3.2.9.

3.2.3.2.6. Validation using an Enterprise RA record

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

3.2.4. Validation of Mailbox Authorization or Control - S/MIME Certificates

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

The CA SHALL verify that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate or has been authorized by the email account holder to act on the account holder's behalf.

The CA SHALL NOT delegate the verification of mailbox authorization or control.

The CA's CP and/or CPS SHALL specify the procedures that the CA employs to perform this verification. CAs SHALL maintain a record of which validation method, including the relevant version number from the TLS Baseline Requirements or S/MIME Baseline Requirements, was used to validate every domain or email address in issued Certificates.

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

Note: Mailbox Fields MAY be listed in Subscriber Certificates using `rfc822Name` or `otherNames` of type `id-on-SmtpUTF8Mailbox` in the `subjectAltName` extension. Mailbox Fields MAY be listed in Subordinate CA Certificates via `rfc822Name` in `permittedSubtrees` within the `nameConstraints` extension.

3.2.4.1. Validating authority over mailbox via domain

The CA MAY confirm the Applicant, such as an Enterprise RA, has been authorized by the email account holder to act on the account holder's behalf by

verifying the entity's control over the domain portion of the Mailbox Address to be used in the Certificate.

The CA SHALL use only the approved methods in Section 3.2.2.4 to perform this verification.

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

3.2.4.2. Validating control over mailbox via email

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

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

The Random Value SHALL be unique in each email. The Random Value SHALL remain valid for use in a confirming response for no more than 24 hours from its creation. The CA MAY specify a shorter validity period for Random Values in its CP and/or CPS.

The Random Value SHALL be reset upon each instance of the email sent by the CA to a Mailbox Address, however all relevant Random Values sent to that Mailbox Address MAY remain valid for use in a confirming response within the validity period described in this Section. In addition, the Random Value SHALL be reset upon first use by the user if intended for additional use as an authentication factor following the Mailbox Address verification.

3.2.4.3. Validating applicant as operator of associated mail server(s)

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

To confirm the Applicant's control of the SMTP FQDN, the CA SHALL use only the currently-approved methods in Section 3.2.2.4.

3.2.4.4. CAA records

This version of the S/MIME Baseline Requirements does not require the CA to check for CAA records. The CAA property tags for `issue`, `issuewild`, and `iodef` as specified in RFC 8659 are not recognized for the issuance of S/MIME Certificates.

3.2.5. Authentication of Organization Identity - S/MIME Certificates

The following requirements SHALL be fulfilled to authenticate Organization identity included in the `Organization-validated` and `Sponsor-validated` profiles.

3.2.5.1. Attribute collection of organization identity

The CA or RA SHALL collect and retain evidence supporting the following identity attributes for the Organization:

1. Formal name of the Legal Entity,
2. A registered Assumed Name for the Legal Entity (if included in the Subject)
3. An organizational unit of the Legal Entity (if included in the Subject)
4. An address of the Legal Entity (if included in the Subject)
5. Jurisdiction of Incorporation or Registration of the Legal Entity, and
6. Unique identifier and type of identifier for the Legal Entity.

The unique identifier SHALL be included in the Certificate `subject:organizationIdentifier` as specified in Section 7.1.4.2.2 and Appendix E.

3.2.5.2. Validation of organization identity

If an Attestation is used as evidence for the validation of the attributes described in this section, then the Attestation SHALL be verified for authenticity as described in Section 3.2.9.

3.2.5.2.1. Verification of name, address, and unique identifier

The CA or RA SHALL verify the full legal name and an address (if included in the Certificate Subject) of the Legal Entity Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Legal Entity's creation, existence, or recognition,
2. A Legal Entity Identifier (LEI) data reference,
3. A site visit by the CA or a third party who is acting as an agent for the CA, or
4. An Attestation which includes a copy of supporting documentation used to establish the Applicant's legal existence, such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act.

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

If an LEI data reference is used, the CA or RA SHALL verify that the RegistrationStatus is ISSUED and the EntityStatus is ACTIVE. The CA SHALL

only allow use of an LEI if the ValidationSources entry is FULLY_CORROBORATED. An LEI SHALL NOT be used if ValidationSources entry is PARTIALLY_CORROBORATED, PENDING, or ENTITY_SUPPLIED_ONLY.

3.2.5.2.2. Verification of assumed name

Applicants MAY request an Assumed Name to be included in the Certificate. The CA or RA SHALL verify that:

1. The Applicant has registered its use of the Assumed Name with the appropriate government agency for such filings in the jurisdiction of its incorporation or registration, and
2. The Assumed Name filing continues to be valid.

The CA MAY rely on an Attestation that indicates the Assumed Name under which the Applicant conducts business, the government agency with which the Assumed Name is registered, and that such filing continues to be valid.

3.2.5.3. Disclosure of verification sources

The CA or RA SHALL verify the unique identifier used in the Certificate from a register that is maintained or authorized by the relevant government agency. The CA SHALL disclose the authorized sources it uses to verify the Applicant's creation, existence, or recognition. This disclosure SHALL be through an appropriate and readily accessible online means. The CA SHALL document where to obtain this information within Section 3.2 of the CA's CP and/or CPS.

Nothing in these Requirements prohibits the use of third-party vendors to obtain regularly-updated and current information from the government register provided that the third party obtains the information directly from the government.

In the case of a LEI data reference, the CA or RA SHALL verify the associated data record with the Global Legal Entity Identifier Foundation (https://search.gleif.org/#/search/).

3.2.6. Non-Verified Subscriber Information

For TLS Certificates:

Issuing CAs SHALL NOT include non-verified Subscriber information in Certificates.

For S/MIME Certificates:

Subscriber information that has not been verified in accordance with these Requirements SHALL NOT be included in Publicly-Trusted S/MIME Certificates.

3.2.7. Validation of Authority

For TLS Certificates:

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.

For S/MIME Certificates:

Before commencing to issue `Organization-validated` and `Sponsor-validated` Certificates for an Applicant, the CA or RA SHALL use a Reliable Method of Communication to verify the authority and approval of an Applicant Representative to perform one or more of the following:

- To act as an Enterprise RA,
- To request issuance or revocation of Certificates, or
- To assign responsibilities to others to act in these roles.

The CA or RA MAY establish a process that allows an Applicant to specify the individuals who may act as Applicant Representatives on an ongoing basis. The CA SHALL provide an Applicant with a list of its authorized Applicant Representatives upon the Applicant's verified written request.

The CA or RA MAY use the sources listed in Section 3.2.5.2.1 to verify the Reliable Method of Communication. Provided that the CA or RA uses a Reliable Method of Communication, the CA or RA 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 or RA deems appropriate.

3.2.8. Criteria for Interoperation

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).

3.2.9. Reliability of Verification Sources - S/MIME Certificates

Before relying on a source of verification data to validate Certificate Requests, the CA SHALL verify its suitability as a Reliable Data Source. Enterprise RA records are a

Reliable Data Source for Individual Subject attributes included in Sponsor-validated Certificates issued to the Enterprise RA's Organization.

The CA or RA MAY rely upon a letter attesting that Subject Information or other fact is correct. The CA or RA SHALL verify that the letter was written by an accountant, lawyer, government official, or other reliable third party in the Applicant's jurisdiction customarily relied upon for such information.

An Attestation SHALL include a copy of documentation supporting the fact to be attested. The CA or RA SHALL use a Reliable Method of Communication to contact the sender and to confirm the Attestation is authentic.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-Key

No stipulation.

3.3.2. Identification and Authentication for Re-Key After Revocation

No stipulation.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

No stipulation.

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 the requirements in this CP.

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 the requirements in this CP. One certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the validation reuse periods, 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

For TLS Certificates:

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 the requirements in this CP and the Issuing CA's CPS. 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.

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, provided that the CA obtained the data or document from a source specified under Section 3.2 or completed the validation itself during the prior periods described below:

- For organization: 824 days,
- For Domain Names and IP Addresses: 397 days,
- For email address: 824 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 TLS Baseline Requirements, a CA may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in this section unless otherwise specifically provided in a CA/Browser Forum 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 the requirements in this CP.

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.

For S/MIME Certificates:

Applicant information SHALL include, but not be limited to, at least one Mailbox Field to be included in the Certificate's `subjectAltName` extension.

Section 6.3.2 limits the validity period of Subscriber Certificates.

The CA MAY reuse completed validations and/or supporting evidence performed in accordance with Section 3.2 within the following limits:

1. **Validation of mailbox authorization or control**: Completed validation of the control of a mail server in accordance with Section 3.2.4.1 or Section 3.2.4.3 SHALL be obtained no more than 398 days prior to issuing the Certificate.

   In the event of changes to the TLS Baseline Requirements methods specified in Section 3.2.4.1, a CA MAY continue to reuse completed validations and/or supporting evidence for the period stated in this section.

   Completed validation of control of a mailbox in accordance with Section 3.2.4.2 SHALL be obtained no more than 30 days prior to issuing the Certificate.

2. **Authentication of organization identity**: Completed validation of organization identity in accordance with Section 3.2.5 SHALL be obtained no more than 825 days prior to issuing the Certificate.

   Validation of authority in accordance with Section 3.2.7 SHALL be obtained no more than 825 days prior to issuing the Certificate, unless a contract between the CA and the Applicant specifies a different term. For example, the contract MAY include the perpetual assignment of roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

3. **Authentication of individual identity**: Completed validation of Individual identity in accordance with Section 3.2.3 SHALL be obtained no more than 825 days prior to issuing the Certificate.

A prior validation SHALL NOT 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.

4.2.2. Approval or Rejection of Certificate Applications

For TLS Certificates:

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.

For S/MIME Certificates:

No Stipulation.

4.2.3. Time to Process Certificate Applications

No Stipulation.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions During Certificate Issuance

Certificate issuance by the Root CA SHALL require at least two individuals 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.

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

No Stipulation.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

Certificate use constitutes its acceptance.

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

For TLS Certificates:

The Root CA MUST disclose, in the CCADB, all Subordinate CA Certificates, issued by the Root CA, that chain up to Root Certificates trusted in Application Software Supplier programs. Disclosure MUST occur within 7 days of Certificate Issuance and prior to issuance of any Certificates under such Subordinate CA Certificate.

Issuing CAs SHALL post TLS Certificates, and/or Precertificates, to Certificate Transparency logs in accordance with then-current Certificate Transparency programs' policies.

For S/MIME Certificates:

No stipulation

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers SHALL use a Private Key associated to a Certificate only for the intended purposes described in Section 1.4 and in accordance with the terms in 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.

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.

4.7.1. 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.

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 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 (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (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 (CRLReason #4, superseded), or
6. The CA is asked by an Application Software Supplier to revoke a Subscriber's Certificate and allowed appeal instances have been exhausted (CRLReason #4, superseded).

The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within five (5) days and use the corresponding CRLReason if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 CRLReason #4, superseded),
2. The CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn),

3. 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),
4. 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, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation),
5. The CA receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the Certificate is no longer legally permitted
6. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn),
7. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn),
8. The CA is made aware that the Certificate was not issued in accordance with the requirements in this CP or the Issuing CA's CPS (CRLReason #4, superseded),
9. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn),
10. The CA's right to issue Certificates under the requirements in this CP 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),
11. Revocation is required by this CP or the Issuing CA's CPS 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),
12. 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),
13. The Private Key used by the CA to issue the Certificate is suspected to have been compromised (CRLReason #1, keyCompromise), or
14. The CA is made aware of a violation of an Application Software Supplier's then-current program requirements, which resulted in the misissuance of

the Certificate (CRLReason #4, superseded).

For TLS Certificates:

Precertificates are in-scope for enforcing compliance with the requirements in this CP. The logging of a Precertificate in a Certificate Transparency log is considered to be a binding intent to issue a final Certificate, as described in section 3.1 of RFC 6962. A final Certificate is "based on" a Precertificate if they have the same serial and issuer, or they have the same serial and the final Certificate's issuer matches the Precertificate's issuer's issuer.

It is mississuance to issue a Certificate based on a Precertificate if they do not exactly match each other according to RFC 6962, section 3.1; and if a Precertificate implies the existence of a Certificate that does not comply with this CP, it is considered misissuance of the Certificate, even if the Certificate does not actually exist.

Effective October 1, 2022:

- An Issuing CA MUST be able to revoke a Certificate presumed to exist, if revocation of the Certificate is required under this CP, even if the final Certificate does not actually exist; and
- An Issuing CA MUST provide CRL and OCSP services and responses in accordance with this CP for all Certificates presumed to exist based on the presence of a Precertificate, even if the Certificate does not actually exist.

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 CP or the Issuing CA's CPS,
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 this CP 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 this CP, or the Issuing CA's CPS.

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, including information on selection of reason codes. The process MUST be described in the Issuing CA's CPS. 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.

When a Subordinate CA Certificate is revoked, the CA SHALL report the revocation to Application Software Suppliers through the CCADB within 30 days of revocation. Additionally, if such revocation is due to a security concern, the CA MUST file a report with Mozilla using their ticketing system (i.e., Bugzilla)

4.9.4. Revocation Request Grace Period

No stipulation.

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

For the status of Subscriber Certificates:

> If the CA publishes a CRL, then the CA SHALL update and reissue CRLs at least once every seven days, and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates:

The CA SHALL update and reissue CRLs at least:

1. once every 365 days, and
2. within 24 hours after revoking a Subordinate CA Certificate.

The value of the nextUpdate field MUST NOT be more than 365 days beyond the value of the thisUpdate field.

4.9.8. Maximum Latency for CRLs

No stipulation.

4.9.9. On-Line Revocation/Status Checking Availability

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 whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

Effective October 1, 2022, the Root CA MUST populate the CCADB fields under "Pertaining to Certificates Issued by This CA" with either the CRL Distribution Point for the "Full CRL Issued By This CA" or a "JSON Array of Partitioned CRLs" for each included Subordinate Certificate chaining up to an included Root Certificate in the Apple Root Program and Mozilla's root store.

4.9.10.On-Line Revocation Checking Requirements

OCSP Responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

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.

For the status of Subscriber Certificates:

1. OCSP responses MUST have a validity interval greater than or equal to eight (8) hours,
2. OCSP responses MUST have a validity interval less than or equal to seven (7) days,
3. For OCSP responses with validity intervals less than sixteen hours, then the CA SHALL update the information provided via OCSP prior to one-half of the validity period before the nextUpdate.
4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA SHALL update the information provided via OCSP at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of Subordinate CA Certificates:

The CA SHALL update information provided via an Online Certificate Status Protocol

1. at least every 365 days, and
2. within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP Responder receives a request for the status of a certificate serial number that is "unused", 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, Section 7.1.2.5, or Section 7.1.5, the responder MUST NOT respond with a "good" status for such requests.

The CA SHOULD monitor the OCSP Responder for requests for "unused" serial numbers as part of its security response procedures.

The OCSP Responder MAY provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC6962].

A Certificate's serial number within an OCSP request is one of the following three options:

1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject, or
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by
    i. the Issuing CA, or
    ii. a Precertificate Signing Certificate], as defined in Section 7.1.2.4, associated with the Issuing CA, or
3. "unused" if neither of the previous conditions are met.

4.9.11. Other Forms of Revocation Advertisements Available

No Stipulation.

4.9.12. Special Requirements re Key Compromise

The Issuing CA's CPS MUST specify the methods that reporters can use to provide evidence of a Private Key compromise. See Section 4.9.1.

4.9.13. Circumstances for Suspension

Issuing CAs MUST NOT support suspension for TLS Certificates.

Issuing CAs MAY support suspension for S/MIME Certificates.

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

4.9.14. Who Can Request Suspension

The Subscriber, RA, or Issuing CA can initiate suspension of S/MIME certificates.

4.9.15. Procedure for Suspension Request

The Issuing CA SHALL document the procedure for suspension in its CPS.

4.9.16. Limits on Suspension Period

No stipulation.

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.

The Issuing CA SHALL support functionality to revoke a Certificate to a specific date. This function SHALL be used only upon a confirmed request by an Application Software Supplier.

4.10.2.Service Availability

The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten (10) 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.Operational Features

No stipulation.

4.11. END OF SUBSCRIPTION

No stipulation.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy and Practices

For S/MIME Certificates:

The CA MAY escrow the Subscriber's Private Key as specified in the CA's CPS.

The CA SHALL notify Subscribers when their Private Keys are escrowed. Escrowed Private Keys SHALL be stored in encrypted form. The CA SHALL protect escrowed Private Keys from unauthorized disclosure.

The CA SHALL recover Subscriber Private Keys only under the circumstances permitted within the CA's CPS.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

The CA/Browser Forum's Network and Certificate System Security Requirements are incorporated in Appendix D.

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 conforms to the requirements in Section 5.4.8. 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 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 CONTROLS

5.1.1. Site Location and Construction

No stipulation.

5.1.2. Physical Access

No stipulation.

5.1.3. Power and Air Conditioning

No stipulation.

5.1.4. Water Exposures

No stipulation.

5.1.5. Fire Prevention and Protection

No stipulation.

5.1.6. Media Storage

No stipulation.

5.1.7. Waste Disposal

No stipulation.

5.1.8. Off-Site Backup

No stipulation.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

No stipulation.

5.2.2. Number of Persons 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

No stipulation.

5.2.4. Roles Requiring Separation of Duties

No stipulation.

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.

5.3.2. Background Check Procedures

No stipulation.

5.3.3. Training Requirements

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 this CP and the Issuing CA's CPS), common threats to the information verification process (including phishing and other social engineering tactics).

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

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

No stipulation.

5.3.7. Independent Contractor Requirements

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

No stipulation.

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 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 this CP.

The CA SHALL record at least the following events:

1. CA certificate and key lifecycle events, including:
    i. Key generation, backup, storage, recovery, archival, and destruction,
    ii. Request of Certificate issuance, renewal, modification, re-key, and revocation,
    iii. Approval and rejection of certificate requests above in Section 5.4.1 (1)(ii),
    iv. Cryptographic device lifecycle management events,
    v. Generation of Certificate Revocation Lists,
    vi. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10), and
    vii. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    i. Request of Certificate issuance, renewal, modification, re-key, and revocation,
    ii. All verification activities stipulated in this CP, and the Issuing CA's CPS,
    iii. Approval and rejection of certificate requests above in Section 5.4.1 (2)(i),
    iv. Issuance of Certificates,
    v. Generation of Certificate Revocation Lists, and
    vi. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).
3. Security events, including:
    i. Successful and unsuccessful PKI system access attempts,
    ii. PKI and security system actions performed,
    iii. Security profile changes,
    iv. Installation, update and removal of software on a Certificate System,
    v. System crashes, hardware failures, and other anomalies,
    vi. Firewall and router activities, and
    vii. Entries to and exits from the CA facility.

Log records MUST include the following elements:

1. Date and time of event,
2. Identity of the person or entity making the journal record, and
3. Description of the event.

5.4.2. Frequency of Processing Audit Log

No stipulation.

5.4.3. Retention Period for Audit Logs

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:
    i. the destruction of the CA Private Key, or
    ii. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key,
2. 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 this CP sets 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 audit log events.

5.4.4. Protection of Audit Log

The CA SHALL implement practices to prevent modification, substitution or deletion of records described in Section 5.4.1 during the retention periods specified in Section 5.4.3.

5.4.5. Audit Log Backup Procedures

No stipulation.

5.4.6. Audit Collection System (Internal Vs. External)

No stipulation.

5.4.7. Notification To Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

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 Issuing CA and each Delegated Third Party SHALL archive the following information:

- Records of the events listed in Section 5.4.1,
- Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems, and
- 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 party SHALL retain, for at least two (2) years:

1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in 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 this CP sets 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

The CA SHALL implement practices to prevent modification, substitution or deletion of archives described in Section 5.5.1 during the retention periods specified in Section 5.5.2.

5.5.4. Archive Backup Procedures

No stipulation.

5.5.5. Requirements for Time-Stamping of Records

No stipulation.

5.5.6. Archive Collection System (Internal or External)

No stipulation.

5.5.7. Procedures to Obtain and Verify Archive Information

No stipulation.

5.6. KEY CHANGEOVER

No stipulation.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

CAs shall have an Incident Response Plan and a Disaster Recovery Plan.

The CA SHALL document 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's plan SHALL include incident management and reporting. The CA SHALL address incident reports as outlined in Section 2.4 of the Mozilla Root Store Policy, and the Microsoft Trusted Root Program's Security Incident Response Requirements.

The CA is not required to publicly disclose its business continuity plan but SHALL make its business continuity 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. Communication strategy to appropriate PKI Participants (e.g., Application Software Suppliers in case of security-sensitive events, Subscribers),
11. 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
12. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
13. What constitutes an acceptable system outage and recovery time,
14. How frequently backup copies of essential business information and software are taken,
15. The distance of recovery facilities to the CA's main site, and
16. 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.

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

No stipulation.

5.7.3. Entity Private Key Compromise Procedures

No stipulation.

5.7.4. Business Continuity Capabilities After a Disaster

No stipulation.

5.8. CA OR RA TERMINATION

No stipulation.

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

1. used as a CA Key Pair for a Root Certificate or
2. 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 for review by the Qualified Auditor.

In all cases, the CA SHALL:

1. generate the CA Key Pair in a physically secured environment as described in the Issuing CA's,
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 Issuing CA's CPS,
4. log its CA Key Pair generation activities,
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CP and/or the Issuing CA's CPS and (if applicable) its Key Generation Script, and
6. generate a new CA Key Pair for each separate Root Certificate.

6.1.1.2. RA Key Pair Generation

No stipulation.

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 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 made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1,
5. The CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

For TLS Certificates:

If the Subscriber Certificate will contain an extKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280], the CA SHALL NOT generate a Key Pair on behalf of a Subscriber, unless the CA is the Subscriber, and SHALL NOT accept a certificate request using a Key Pair previously generated by the CA.

For S/MIME Certificates:

The CA or a Delegated Third Party MAY generate the Private Key on behalf of the Subscriber.

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.

When the CA or any of its designated RAs generates the Private Key on behalf of the Subscriber then the CA SHALL encrypt the Private Key for transport to the Subscriber. The encryption SHALL be commensurate in strength to the Private Key being protected.

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.

For S/MIME Certificates:

If the CA or a Delegated Third Party generates the Private Key on behalf of the Subscriber where the Private Keys will be transported to the Subscriber, then the entity generating the Private Key SHALL either transport the Private Key in hardware with an activation method that is equivalent to 128 bits of encryption or encrypt the Private Key with at least 128 bits of encryption strength. Example methods include using a 128-bit AES key to wrap the Private Key or storing the key in a PKCS 12 file encrypted with a randomly generated password of more than 16 characters containing uppercase letters, lowercase letters, numbers, and symbols for transport. The CA or Delegated Third Party SHALL NOT store Subscriber Private Keys in clear text.

The material used to activate/protect the Private Key (e.g., a password used to secure a PKCS 12 file) must be delivered to the Subscriber securely and separately from the container holding the Private Key.

6.1.3. Public Key Delivery to Certificate Issuer

No stipulation.

6.1.4. CA Public Key Delivery to Relying Parties

No stipulation.

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 Private Keys, part of CA Key Pairs, outside the validated system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Keys. The CA SHALL encrypt its Private Keys 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

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.

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

CAs SHALL employ multiple individuals in Trusted Roles, and in all cases not fewer than two (2), in a physically secured environment to generate CA Key Pairs and when Private Keys are activated for signature operations.

6.2.3. Private Key Escrow

Issuing CAs SHALL not escrow Private Keys associated with Root or Subordinate CA Certificates.

Issuing CAs MAY escrow Subscriber's Private Keys in S/MIME Certificates with keyUsage and extKeyUsage values indicated in Section 7.1.2.3. Issuing CAs SHALL obtain Subscriber's authorization prior to escrowing a Private Key.

6.2.4. Private Key Backup

Issuing CAs SHALL backup, store and recover Private Keys, associated to Root and Subordinate CA Certificates, in compliance with Section 6.2.2.

6.2.5. Private Key Archival

Parties other than the Subordinate CA SHALL NOT archive the Subordinate CA Private Keys unless the Subordinate CA provides authorization.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

All CA Key Pairs SHALL be generated and stored within a cryptographic module meeting the requirements in Section 6.2.1. For backup purposes, Private Keys may be transferred between cryptographic modules. Transfer procedures SHALL ensure that Private Keys are never disclosed.

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

CA's Private Keys, including their backups, SHALL be stored in cryptographic modules that meet the specifications in Section 6.2.1.

6.2.8. Method of Activating Private Key

No stipulation.

6.2.9. Method of Deactivating Private Key

No stipulation.

6.2.10. Method of Destroying Private Key

No stipulation.

6.2.11. Cryptographic Module Rating

Cryptographic modules SHALL meet the specifications in Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

Issuing CAs SHALL archive Public Keys in compliance with Section 5.5..

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

When issuing Certificates, Issuing CAs SHALL use the Certificate lifespans below. Certificate operational periods and Key Pair usage period are the same except where explicitly differentiated.

For Root Certificates:

Not to exceed 9,125 days (25 years)

For Subordinate CA Certificates:

Not to exceed 5,475 days (15 years)

For Subscriber TLS Certificates:

- containing id-kp-serverAuth: Not to exceed 397 days

For Subscriber S/MIME Certificates:Strict and Multipurpose: Not to exceed 824 days

For OCSP Responder or other administrative Certificates:

- containing id-kp-OCSPSigning:
- Issued by a Root CA: Not to exceed 180 days
- Issued by a subordinate CA: Not to exceed 60 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, Certificates SHOULD NOT be issued for the maximum permissible time by default, in order to account for such adjustments.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

No stipulation.

6.4.2. Activation Data Protection

No stipulation.

6.4.3. Other Aspects of Activation Data

No stipulation.

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

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

No stipulation.

6.6.2. Security Management Controls

No stipulation.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

No stipulation.

6.8. TIME-STAMPING

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

The CA SHALL meet the technical requirements set forth in Section 2.2 - Publication of Information, Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking.

For TLS Certificates:

Prior to 2023-09-15, the CA SHALL issue Certificates in accordance with the profile specified in these Requirements or the profile specified in version 1.8.6 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. Effective 2023-09-15, the CA SHALL issue Certificates in accordance with the profile specified in these Requirements.

7.1.1. Version Numbers

Certificates MUST be of type X.509 v3.

7.1.2. Certificate Content and Extensions

If the CA asserts compliance with the 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 the Baseline Requirements. 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 7.1.2.12 - S/MIME Subordinate CA Certificate Profile
  - Section 7.1.2.7 - Subscriber (Server) Certificate Profile

- Section 7.1.2.13 - S/MIME Subscriber 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)
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	Encoding, length and order is specified in Section 7.1.4.2. Common Name structure is specified in 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
Signed Certificate Timestamp List	MAY	No	See Section 7.1.2.11.3
basicConstraints	MUST	Yes	See Section 7.1.2.1.4
KeyUsage	MUST	Yes	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	No	See Section 7.1.2.11.4 S/MIME: SHALL contain a value that is included in the `keyIdentifier` field of the `authorityKeyIdentifier` extension in Certificates issued by the Root CA.
extKeyUsage	MUST NOT	-	-
certificatePolicies	TLS: NOT RECOMMENDED S/MIME: MUST NOT	No -	See Section 7.1.2.10.5
authorityKeyIdentifier	RECOMMENDED	No	See Section 7.1.2.1.3
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	TLS: NOT RECOMMENDED S/MIME: MUST NOT be present

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 the Baseline Requirements and this CP 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
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	No	See Section 7.1.2.11.1
basicConstraints	MUST	Yes	See Section 7.1.2.10.4
certificatePolicies	MUST	No	See Section 7.1.2.10.5
crlDistributionPoints	MUST	No	See Section 7.1.2.11.2
keyUsage	MUST	Yes	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	No	See Section 7.1.2.11.4
authorityInformationAccess	SHOULD	No	See Section 7.1.2.10.3
nameConstraints	MAY	(Note 1)	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	No	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Note 1: See Section 7.1.2.10.8 for further requirements, including regarding criticality of this extension.

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 (Note 1)	No	See Section 7.1.2.2.4

Note 1: 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.

Cross-Certified Subordinate CA with Restricted EKU

Extension	Presence	Critical	Description
extKeyUsage	MUST (Note 1)	No	See Section 7.1.2.2.5

Note 1: 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.

7.1.2.2.4. Cross-Certified Subordinate CA Extended Key Usage - Unrestricted

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

Field	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.

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)

Key Purpose	Description
id-kp-serverAuth id-kp-	MUST be present
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 Ex- tended Key Usage Purposes (i.e., for restricted Cross-Certified Subordinate CAs not issuing TLS certificates directly or transitively)

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:
    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.

7.1.2.3. 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	No	See Section 7.1.2.11.1
basicConstraints	MUST	Yes	See Section 7.1.2.10.3
crlDistributionPoints	MUST	No	See Section 7.1.2.11.2
keyUsage	MUST	Yes	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	No	See Section 7.1.2.11.4
extKeyUsage	MUST (Note1)	No	See Section 7.1.2.3.3
authorityInformationAccess	SHOULD	No	See Section 7.1.2.10.3

Extension	Presence	Critical	Description
certificatePolicies	MAY	No	See Section 7.1.2.3.2
nameConstraints	MAY	(Note 2)	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	No	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Note 1: 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.

Note 2: See Section 7.1.2.10.8 for further requirements, including regarding criticality of this extension.

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

Policy Restricted

Field	Presence	Contents
policyIdentifier	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST NOT	
anyPolicy	MUST NOT	The anyPolicy Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be defined and documented in the Issuing CA's CPS.

Field	Presence	Contents
policyQualifiers	NOT RECOMMENDED	If present, MUST contain only permitted policyQualifiers from the table below.

Permitted policyQualifiers

Field	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.

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	-

7.1.2.4.1. Technically Constrained Precertificate Signing CA Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	No	See Section 7.1.2.11.1
basicConstraints	MUST	Yes	See Section 7.1.2.10.4
certificatePolicies	MUST	No	See Section 7.1.2.10.5
crlDistributionPoints	MUST	No	See Section 7.1.2.11.2
keyUsage	MUST	Yes	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	No	See Section 7.1.2.11.4
extKeyUsage	MUST (Note 1)	No	See Section 7.1.2.4.2

Extension	Presence	Critical	Description
authorityInformationAccess	SHOULD	No	See Section 7.1.2.10.3
nameConstraints	MAY	(Note 2)	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	No	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Note 1: 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.

Note 2: See Section 7.1.2.10.8 for further requirements, including regarding criticality of this extension.

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.

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

Field	Description
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	No	See Section 7.1.2.11.1
basicConstraints	MUST	Yes	See Section 7.1.2.10.4
certificatePolicies	MUST	No	See Section 7.1.2.10.5
crlDistributionPoints	MUST	No	See Section 7.1.2.11.2
keyUsage	MUST	Yes	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	No	See Section 7.1.2.11.4
extKeyUsage	MUST (Note1)	No	See Section 7.1.2.10.6
nameConstraints	MUST	(Note 2)	See Section 7.1.2.5.2
authorityInformationAccess	SHOULD	No	See Section 7.1.2.10.3
Signed Certificate Timestamp List	MAY	No	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Note 1: 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.

Note 2: See Section 7.1.2.10.8 for further requirements, including regarding criticality of this extension.

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.
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.

Name Type	Presence	Permitted Subtrees	Excluded Subtrees	Entire Namespace Exclusion
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 asignee'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 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

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.

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 7.1.2.6.1
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	No	See Section 7.1.2.11.1
basicConstraints	MUST	Yes	See Section 7.1.2.10.4
certificatePolicies	MUST	No	See Section 7.1.2.10.5
crlDistributionPoints	MUST	No	See Section 7.1.2.11.2

Extension	Presence	Critical	Description
keyUsage	MUST	Yes	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	No	See Section 7.1.2.11.4
extKeyUsage	MUST (Note 1)	No	See Section 7.1.2.10.6
authorityInformationAccess	SHOULD	No	See Section 7.1.2.10.3
nameConstraints	MAY	(Note 2)	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	No	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Note 1: 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.

Note 2: See Section 7.1.2.10.8 for further requirements, including regarding criticality of this extension.

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	See Section 7.1.2.10.1
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).

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

Field	Presence	Value	Verification
countryName	MAY	The two-letter ISO 3166-1 country code for the country Section 3.2.2.3 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

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

Field	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
organizationName	NOT RECOMMENDED	If present, MUST contain the Subject's name or DBA.	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

Field	Presence	Value	Verification
organizationalUnitName	NOT RECOMMENDED	-	-
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.
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

Field	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 3.2.2.3
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 3.2.2.1
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

Field	Presence	Value	Verification
organizationName	MUST	The Subject'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
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 9.2.
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.

7.1.2.7.6. Subscriber Certificates CA Extensions

Extension	Presence	Critical	Description
authorityInformationAccess	MUST	No	See Section 7.1.2.7.7
authorityKeyIdentifier	MUST	No	See Section 7.1.2.11.1
certificatePolicies	MUST	No	See Section 7.1.2.7.9
extKeyUsage	MUST	No	See Section 7.1.2.7.10
subjectAltName	MUST	(Note 1)	See Section 7.1.2.7.12
nameConstraints	MUST NOT	-	-
keyUsage	SHOULD	Yes	See Section 7.1.2.7.11
basicConstraints	MAY	Yes	See Section 7.1.2.7.8
crlDistributionPoints	MAY	No	See Section 7.1.2.11.2
Signed Certificate Timestamp List	MAY	No	See Section 7.1.2.11.3
subjectKeyIdentifier	NOT RECOMMENDED	No	See Section 7.1.2.11.4
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Note 1: 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.

7.1.2.7.7. Subscriber Certificate Authority Information Access

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	OID	Access Location	Presence	Maximum	Description
id-ad-ocsp	1.3.6.1.5.5.7.48.1	uniformResourceIdentifier	MUST	*	A HTTP URL of the Issuing CA's OCSP responder.
id-ad-calssuers	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 Issuing CA's CPS.
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 Section 7.1.6.1). Regardless of the order of PolicyInformation values, the Certificate Policies extension MUST contain exactly one Reserved Certificate Policy Identifier.

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.

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.

Key Usage for RSA Public Keys

Key Usage	Permitted	Required
digitalSignature	Yes	SHOULD
nonRepudiation	No	-
keyEncipherment	Yes	MAY
dataEncipherment	Yes	NOT RECOMMENDED
keyAgreement	No	-
keyCertSign	No	-
cRLSign	No	-
encipherOnly	No	-
decipherOnly	No	-

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	Yes	MUST
nonRepudiation	No	-
keyEncipherment	No	-
dataEncipherment	No	-
keyAgreement	Yes	NOT RECOMMENDED
keyCertSign	No	-
cRLSign	No	-
encipherOnly	No	-
decipherOnly	No	-

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).

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	No	-
rfc822Name	No	-
dNSName	Yes	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. 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	No	-
directoryName	No	-
ediPartyName	No	-
uniformResourceIdentifier	No	-
iPAddress	Yes	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 Section 3.2.2.5. The entry MUST NOT contain a Reserved IP Address.
registeredID	No	-

7.1.2.8. OCSP Responder 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	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 Certificate Validity

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

7.1.2.8.2. OCSP Responder Certificate Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	No	See Section 7.1.2.11.1
extKeyUsage	MUST	-	See Section 7.1.2.8.5
id-pkix-ocsp-nocheck	MUST	No	See Section 7.1.2.8.6
keyUsage	MUST	Yes	See Section 7.1.2.10.7
basicConstraints	MAY	Yes	See Section 7.1.2.8.4
nameConstraints	MUST NOT	-	-
subjectAltName	MUST NOT	-	-
subjectKeyIdentifier	SHOULD	No	See Section 7.1.2.11.4
authorityInformationAccess	NOT RECOMMENDED	No	See Section 7.1.2.8.3
certificatePolicies	MUST NOT	No	See Section 7.1.2.8.8
crlDistributionPoints	MUST NOT	No	See Section 7.1.2.11.2
Signed Certificate Timestamp List	MAY	No	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-calssuers. 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 AuthorityInformationAccesssSyntax MUST contain one or more AccessDescriptions. Each AccessDescription MUST only contain a permitted accessMethod, as detailed below, and each AuthorityInfoAccessSyntax MUST contain all required AccessDescriptions.

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

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 Certificate 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 Certificate Key Usage

Key Usage	Permitted	Required
digitalSignature	Yes	Yes
nonRepudiation	No	-
keyEncipherment	No	-
dataEncipherment	No	-
keyAgreement	No	-
keyCertSign	No	-
cRLSign	No	-
encipherOnly	No	-
decipherOnly	No	-

7.1.2.8.8. OCSP Responder 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	NOT RECOMMENDED	-
anyPolicy	NOT RECOMMENDED	-
Any other identifier	NOT RECOMMENDED	If present, MUST be defined and documented in the Issuing CA's CPS.
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	-	-

Note 1: See Section 7.1.2.8.2 for applicable effective dates for when this extension may be included.

Note 2: 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 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.

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
subjectUniqueID	Encoded value MUST be byte-for-byte identical to the subjectUniqueID field of the Certificate
extensions	See Section 7.1.2.9.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the
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
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

Field	Description
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	Yes	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, 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	Yes	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
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.

For S/MIME Certificates:

All fields and extensions SHALL be set in accordance with RFC 5280. The CA SHALL NOT issue a Certificate that contains a `keyUsage` flag, `extKeyUsage` value, Certificate extension, or other data not specified in Section 7.1.2.2, Section 7.1.2.12, or Section 7.1.2.13 unless the CA is aware of a reason for including the data in the Certificate. If the CA includes fields or extensions in a Certificate that are not specified but are otherwise permitted by this CP, then the CA SHALL document the processes and procedures that the CA employs for the validation of information contained in such fields and extensions in its CPS.

CAs SHALL NOT issue a Certificate with:

1. Extensions that do not apply in the context of the public Internet (such as an `extKeyUsage` value for a service that is only valid in the context of a privately managed network), unless:
    i. Such value falls within an OID arc for which the Applicant demonstrates ownership, or
    ii. The Applicant can otherwise demonstrate the right to assert the data in a public context, or
2. Field or extension values which have not been validated according to the processes and procedures described in the S/MIME Requirements, this CP, and/or the CA's CPS.

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
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 3.2.2.1
organizationalUnitName	MUST NOT / SHOULD NOT (Note 1)	-	-
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

Note 1: 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 SHOULD NOT be included in other types of CA Certificates.

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	OID	Access Location	Presence	Minimum	Description
id-ad-ocsp	1.3.6.1.5.5.7.48.1	uniformResourceIdentifier	SHOULD	*	A HTTP URL of the Issuing CA's OCSP responder.
id-ad-calssuers	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.

7.1.2.10.4. CA Certificate Basic Constraints

Field	Description
cA	MUST be 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, 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	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) 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 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 Section 7.1.6.1). Regardless of the order of PolicyInformation values, the Certificate Policies extension MUST contain exactly one Reserved Certificate Policy Identifier.

Although RFC 5280 allows PolicyInformations to appear in any order, several client implementations have implemented logic that consideres 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.

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
Any other value	-	NOT RECOMMENDED

7.1.2.10.7. CA 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.

Key Usage for RSA Public Keys

Key Usage	Permitted	Required
digitalSignature	Yes	No (Note 1)
nonRepudiation	No	-
keyEncipherment	No	-
dataEncipherment	No	-
keyAgreement	No	-
keyCertSign	Yes	Yes
cRLSign	Yes	Yes
encipherOnly	No	-
decipherOnly	No	-

Note 1: 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.

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. See following table.
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
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.

Name Type	Presence	Permitted Subtrees	Excluded Subtrees
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 asignee'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.
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. 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.

For S/MIME Certificates:

All fields and extensions SHALL be set in accordance with RFC 5280. The CA SHALL NOT issue a Certificate that contains a `keyUsage` flag, `extKeyUsage` value, Certificate extension, or other data not specified in Section 7.1.2.2, Section 7.1.2.12, or Section 7.1.2.13 unless the CA is aware of a reason for including the data in the Certificate. If the CA includes fields or extensions in a Certificate that are not specified but are otherwise permitted by this CP, then the CA SHALL document the processes and procedures that the CA employs for the validation of information contained in such fields and extensions in its CPS.

CAs SHALL NOT issue a Certificate with:

1. Extensions that do not apply in the context of the public Internet (such as an `extKeyUsage` value for a service that is only valid in the context of a privately managed network), unless:
    i. Such value falls within an OID arc for which the Applicant demonstrates ownership, or
    ii. The Applicant can otherwise demonstrate the right to assert the data in a public context, or
2. Field or extension values which have not been validated according to the processes and procedures described in the S/MIME Requirements, this CP, and/or the CA's CPS.

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 Point

If 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 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.

7.1.2.12. S/MIME 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.
signature	See Section 7.1.3.2
issuer	Encoded value MUST be byte-for-byte identical to the encoded subject
validity	See Section 6.3.2
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 7.1.2.12.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.12.1. S/MIME Subordinate CA Extensions

Extension	Presence	Critical	Description
certificatePolicies	MUST	No	See Section 7.1.2.12.2
authorityKeyIdentifier	MUST	No	See Section 7.1.2.12.3
basicConstraints	MUST	Yes	See Section 7.1.2.12.4

Extension	Presence	Critical	Description
extKeyUsage	(Note 2)	No	See Section 7.1.2.12.5
keyUsage	MUST	Yes	See Section 7.1.2.10.7
nameConstraints	MAY	SHOULD (Note 1)	See Section 7.1.2.10.8
subjectKeyIdentifier	MUST	No	See Section 7.1.2.11.4 SHALL contain a value that is included in the `keyIdentifier` field of the `authorityKeyIdentifier` extension in Certificates issued by the Root CA
cRLDistributionPoints	MUST	No	See Section 7.1.2.11.2
authorityInformationAccess	SHOULD	No	See Section 7.1.2.10.3 SHOULD contain the HTTP URL of the Issuing CA Certificate (accessMethod `id-ad-caIssuers` = 1.3.6.1.5.5.7.48.2). MAY contain the HTTP URL of the Issuing CA OCSP responder (accessMethod `id-ad-ocsp` = 1.3.6.1.5.5.7.48.1).
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Note 1: Non-critical Name Constraints are an exception to RFC 5280 (4.2.1.10), however, they MAY be used until the `nameConstraints` extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.

Note 2: MAY be present for Cross Certificates; SHALL be present otherwise.

For Cross Certificates that share a Subject Distinguished Name and Subject Public Key with a Root CA Certificate operated in accordance with these Requirements, this extension MAY be present. If present, this extension SHOULD NOT be marked critical. This extension SHALL only contain usages for which the Issuing CA has verified the Cross Certificate is authorized to assert. This extension SHALL NOT contain the anyExtendedKeyUsage usage.
For all other Subordinate CA Certificates, including Technically Constrained Subordinate CA Certificates, this extension SHALL be present and SHOULD NOT be marked critical.

While RFC 5280, Section 4.2.1.12, notes that this extension will generally only appear within end-entity Certificates, S/MIME 1.0 Baseline Requirements make use of this extension to further protect relying parties by limiting the scope of Subordinate Certificates, as implemented by a number of Application Software Suppliers.

7.1.2.12.2. S/MIME Subordinate CA Certificate Policies

All `policyIdentifier`s included in this extension SHALL be included in accordance with Section 7.1.6.3.

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 Issuing CA's CPS.
policyQualifiers	MAY	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 Section 7.1.6.1). Regardless of the order of PolicyInformation values, the Certificate Policies extension MUST contain exactly one Reserved Certificate Policy Identifier.

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.

Permitted PolicyInformation Qualifiers

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.
`id-qt-unotice` (OID:	MAY	-	If present, SHALL contain `explicitText` and SHALL NOT contain `noticeRef`.

7.1.2.12.3. S/MIME Subordinate CA Authority Key Identifier

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

7.1.2.12.4. S/MIME Subordinate CA Basic Constraints

Field	Description
cA	MUST be set TRUE
pathLenConstraint	MAY be present

7.1.2.12.5. S/MIME Subordinate CA Certificate Extended Key Usage

Key Purpose	OID	Presence
id-kp-emailProtection	1.3.6.1.5.5.7.3.4	MUST
id-kp-serverAuth	1.3.6.1.5.5.7.3.1	MUST NOT
id-kp-codeSigning	1.3.6.1.5.5.7.3.3	MUST NOT
id-kp-timeStamping	1.3.6.1.5.5.7.3.8	MUST NOT
anyExtendedKeyUsage	2.5.29.37.0	MUST NOT
Any other value	-	MAY

7.1.2.13. S/MIME Subscriber 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	Encoded value MUST be byte-for-byte identical to the encoded subject
validity	See Section 6.3.2
subject	See Section 7.1.2.10.2

Field	Description
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.13.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.13.1. S/MIME Subscriber Certificate Extensions

Extension	Presence	Critical	Description
certificatePolicies	MUST	No	See Section 7.1.2.13.2
authorityKeyIdentifier	MUST	No	See Section 7.1.2.13.3
basicConstraints	MAY	-	See Section 7.1.2.13.4
extKeyUsage	(Note 2)	No	See Section 7.1.2.13.5
keyUsage	MUST	Yes	See Section 7.1.2.13.6
subjectKeyIdentifier	SHOULD	No	SHOULD contain a value that is derived from the Public Key included in the Subscriber Certificate.
cRLDistributionPoints	MUST	No	See Section 7.1.2.11.2
authorityInformationAccess	SHOULD	No	See Section 7.1.2.10.3 SHOULD contain the HTTP URL of the Issuing CA Certificate (accessMethod `id-ad-caIssuers` = 1.3.6.1.5.5.7.48.2). MAY contain the HTTP URL of the Issuing CA OCSP responder (accessMethod `id-ad-ocsp` = 1.3.6.1.5.5.7.48.1).
subjectAlternativeName	MUST	No	This extension SHOULD NOT be marked critical unless the subject field is an empty sequence. The value of this extension SHALL be encoded as specified in Section 7.1.4.2.1.

Extension	Presence	Critical	Description
smimeCapabilities	MAY	No	May indicate cryptographic capabilities of the sender of a signed S/MIME message, defined in RFC 4262.
subjectDirectoryAttributes	MUST NOT	No	This extension is used to contain verified attributes which are not part of the Subject's Distinguished Name such as dateOfBirth, placeOfBirth, gender, countryOfCitizenship, or countryOfResidence in accordance with RFC 3739 Section 3.2.2.
qcStatements	MAY	No	Indicates a Certificate that is issued as Qualified within a defined legal framework from an identified country or set of countries in accordance with RFC 3739 Section 3.2.6 and/or ETSI EN 319 412-5, Section 4.
Legal Entity Identifier - Mailbox-validated	MUST NOT	-	-
Legal Entity Identifier - Organization-validated	MAY	No	LEI (1.3.6.1.4.1.52266.1) The Legal Entity Identifier (LEI) is a 20-character, alpha-numeric code used in accordance with ISO 17442-1:2020, Clause 6 and ISO 17442-2:2020, Clause 4. The CA SHALL verify that the RegistrationStatus for the LEI record is ISSUED and the EntityStatus is ACTIVE. The CA SHALL only allow use of an LEI if the ValidationSources entry is FULLY_CORROBORATED. An LEI SHALL NOT be used if ValidationSources entry is PARTIALLY_CORROBORATED, PENDING, or ENTITY_SUPPLIED_ONLY.
Adobe Extensions	MUST NOT	-	-
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.13.2. S/MIME Subscriber CA Certificate Policies

All `policyIdentifier`s included in this extension SHALL be included in accordance with Section 7.1.6.4.

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 Issuing CA's CPS.
policyQualifiers	MAY	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 Section 7.1.6.1). Regardless of the order of PolicyInformation values, the Certificate Policies extension MUST contain exactly one Reserved Certificate Policy Identifier.

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.

Permitted PolicyInformation Qualifiers

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.
`id-qt-unotice` (OID:	MAY	-	If present, SHALL contain `explicitText` and SHALL NOT contain `noticeRef`.

7.1.2.13.3. S/MIME Subscriber Certificate Authority Key Identifier

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

7.1.2.13.4. S/MIME Subscriber Certificate Basic Constraints

Field	Description
cA	MUST NOT be set TRUE
pathLenConstraint	MUST NOT be present

7.1.2.13.5. S/MIME Subscriber Certificate Extended Key Usage

Key Purpose	OID	Presence
id-kp-emailProtection	1.3.6.1.5.5.7.3.4	MUST
id-kp-serverAuth	1.3.6.1.5.5.7.3.1	Strict: MUST NOT Multipurpose: MAY
id-kp-codeSigning	1.3.6.1.5.5.7.3.3	Strict: MUST NOT
id-kp-timeStamping	1.3.6.1.5.5.7.3.8	MUST NOT
anyExtendedKeyUsage	2.5.29.37.0	MUST NOT
Any other value	-	Strict: MUST NOT Multipurpose: MAY

7.1.2.13.6. S/MIME 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.

Bit positions other than those listed below MUST NOT be set.

Key Usage for RSA Public Keys - Strict

Key Usage	Signing Only	Key Management Only	Dual Use
digitalSignature	MUST	-	MUST
nonRepudiation	MAY	-	MAY
keyEncipherment	-	MUST	MUST

Key Usage for RSA Public Keys - Multipurpose

Key Usage	Signing Only	Key Management Only	Dual Use
digitalSignature	MUST	-	MUST
nonRepudiation	MAY	-	MAY
keyEncipherment	-	MUST	MUST
dataEncipherment	-	MAY	MAY

Key Usage for ECC Public Keys

Key Usage	Signing Only	Key Management Only	Dual Use
digitalSignature	MUST	-	MUST
nonRepudiation	MAY	-	MAY
keyAgreement	-	MUST	MUST
encipherOnly	-	MAY	MAY (if `keyAgreement` is set)
decipherOnly	-	MAY	MAY (if `keyAgreement` is set)

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-384keys, 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
- The signature Algorithm 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:
304106092a864886f70d01010a3034a00f300d060960864801650
30402010500a11c301a06092a864886f70d010108300d06096086
4801650304020105 00a203020120.

- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes:
  Encoding:
  304106092a864886f70d01010a3034a00f300d060960864801650
  30402020500a11c301a06092a864886f70d010108300d06096086
  4801650304020205 00a203020130
- RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:
  Encoding:
  304106092a864886f70d01010a3034a00f300d060960864801650
  30402030500a11c301a06092a864886f70d010108300d06096086
  4801650304020305 00a203020140

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.

Attribute values SHALL be encoded according to RFC 5280.

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 included certificates issued by such CA Certificates, as they are out of the Baseline Requirement and this CP.

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.
    - 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 (Note 1)
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
surname	2.5.4.4	RFC 5280	MUST use UTF8String or PrintableString	64 (Note 2)
givenName	2.5.4.42	RFC 5280	MUST use UTF8String or PrintableString	64 (Note 2)
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 1: ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits.

Note 2: 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.

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 (Note 1)
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

Attribute	OID	Specification	Encoding Requirements	Max Length (Note 1)
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
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 1: ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits.

For S/MIME Certificates:

CAs SHALL NOT include a Mailbox Address in a Mailbox Field except as verified in accordance with Section 3.2.2.

Subject attributes SHALL 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.

7.1.4.2.1. S/MIME Subject alternative name extension

Extension	Required/ Optional	Description
subjectAltName	MUST	This extension SHALL contain at least one `GeneralName` entry of the following types: · `rfc822Name` and/or · `otherName` of type `id-on-SmtpUTF8Mailbox`, encoded in accordance with RFC 8398

All Mailbox Addresses in the subject field or entries of type `dirName` of this extension SHALL be repeated as `rfc822Name` or `otherName` values of type `id-on-SmtpUTF8Mailbox` in this extension.

The CA MAY include `GeneralName` entries of type `dirName` provided that the information contained in the `Name` complies with the requirements set forth in the appropriate subsection of Section 7.1.4.2.2 according to the Certificate Type. Additionally, information contained in the `Name` SHALL be validated according to Section 3.1, Section 3.2.5, and/or Section 3.2.3, as appropriate for the Certificate Type.

ForMultipurpose Generation profiles, then the CA MAY include `otherName` entries of any type, provided that the CA has validated the field value according to its CP and/or CPS.

The CA SHALL NOT include `GeneralName` entries that do not conform to the requirements of this section.

7.1.4.2.2. S/MIME Subject distinguished name fields

Field	OID	Description
commonName	2.5.4.3	If present, this field SHALL contain one of the following values verified in accordance with Section 3.2. • Mailbox-validated: Mailbox Address • Organization-validated: `organizationName` or Mailbox Address • Sponsor or Individual-validated: Personal Name, Pseudonym, or Mailbox Address If present, the Personal Name SHALL contain a name of the Subject. The Personal Name SHOULD be presented as `givenName` and/or `surname`. The Personal Name MAY be in the Subject's preferred presentation format or a format preferred by the CA or Enterprise RA, but SHALL be a meaningful representation of the Subject's name as verified under Section 3.2.3. If present, the Mailbox Address SHALL contain a `rfc822Name` or `otherName` value of type `id-on-SmtpUTF8Mailbox` from `extensions:subjectAltName`. If present, the Pseudonym SHALL contain the `pseudonym` if that Subject attribute is also present. Note: Like all other Certificate attributes, `commonName` and `emailAddress` SHALL comply with the attribute upper bounds defined in RFC 5280. Additional specifications for naming are provided in Section 3.1.
organizationName	2.5.4.10	If present, the CA SHALL confirm that the organizationalUnitName is the full legal organization name of an Affiliate of the organizationName in the Certificate and has been verified in accordance with the requirements of Section 3.2.5. 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.

Field	OID	Description
organizationIdentifier	2.5.4.97	If present, this field SHALL contain a Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme. The organizationIdentifier SHALL be encoded as a PrintableString or UTF8String. The Registration Scheme identified in the Certificate SHALL be the result of the verification performed in accordance with Section 3.2.5. The Registration Scheme SHALL be identified using the following structure in the presented order: • 3 character Registration Scheme identifier, • 2 character ISO 3166 country code for the nation in which the Registration Scheme is operated, or if the scheme is operated globally ISO 3166 code "XG" SHALL be used, • For the NTR Registration Scheme identifier, where registrations are administrated at the subdivision (state or province) level, a plus "+" (0x2B (ASCII), U+002B (UTF-8)) followed by an up-to-three alphanumeric character ISO 3166-2 identifier for the subdivision of the nation in which the Registration Scheme is operated, • a hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)), • Registration Reference allocated in accordance with the identified Registration Scheme. See Notes 1 and 2 below.
givenName and/or surname	2.5.4.42 2.5.4.4	If present, this field SHALL contain a Natural Person Subject's name as verified under Section 3.2.3. Subjects with a single legal name SHALL provide the name in the subject:surname attribute. The subject:givenName and/or subject:surname SHALL NOT be present if the subject:pseudonym is present.
pseudonym	2.5.4.65	If present, this field SHALL NOT be present if the subject:givenName and/or subject:surname are present. If present, the subject:pseudonym field SHALL be verified according to Section 3.1.3.
serialNumber	2.5.4.5	If present, this field MAY be used to contain an identifier assigned by the CA or RA to identify and/or to disambiguate the Subscriber. In addition, this field MAY be used in the Sponsor-validated and Individual-validated profiles to contain a Natural Person Identifier as described in ETSI EN 319 412-1 Section 5.1.3. Registration Schemes listed in Appendix E are recognized as valid under these Requirements. The CA SHALL confirm that the Individual represented by the Natural Person Identifier is the same as the Certificate Subject in accordance with Section 3.2.3.
emailAddress	1.2.840.113549.1.9.1	If present, this field SHALL contain a single Mailbox Address as verified under Section 3.2.2.

Field	OID	Description
title	2.5.4.12	If present, this field SHALL contain only a organizational role/ title or a regulated professional designation verified according to Section 3.2.3.
streetAddress (Number and street)	2.5.4.9	If present, this field SHALL contain the Subject's street address information as verified under Section 3.2.5 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.3 for Individual-validated Certificate Types.
localityName	2.5.4.7	If present, this field SHALL contain the Subject's locality information as verified under Section 3.2.3 for Organization-validated and Sponsor-validated Certificate Types or Individual-validated Certificate Types. If the countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2, the localityName field MAY contain the Subject's locality and/or state or province information.
stateOrProvinceName	2.5.4.8	If present, this field SHALL contain the Subject's state or province information as verified under Section 3.2.5 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.3 for Individual-validated Certificate Types. If the countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2, the stateOrProvinceName field MAY contain the full name of the Subject's country information.
postalCode	2.5.4.17	If present, this field SHALL contain the Subject's zip or postal information as verified under Section 3.2.5 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.3 for Individual-validated Certificate Types.
countryName	2.5.4.6	If present, this field SHALL contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.5 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.3 for Individual-validated Certificate Types. If a Country is not represented by an official ISO 3166-1 country code, the CA MAY specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

Note 1: Registration References MAY contain hyphens but Registration Schemes, ISO 3166 country codes, and ISO 3166-2 identifiers do not. Therefore if more than one hyphen appears in the structure, the leftmost hyphen is a separator, and the remaining hyphens are part of the Registration Reference.

For example:

- NTRGB-12345678 (NTR scheme, Great Britain, Unique Identifier at Country level is 12345678).
- NTRUS+CA-12345678 (NTR Scheme, United States - California, Unique identifier at State level is 12345678).

- VATDE-123456789 (VAT Scheme, Germany, Unique Identifier at Country Level is 12345678).
- PSDBE-NBB-1234.567.890 (PSD Scheme, Belgium, NCA's identifier is NBB, Unique Identifier assigned by the NCA is 1234.567.890).

Registration Schemes listed in Appendix E are recognized as valid under these Requirements. The CA SHALL:

- Confirm that the organization represented by the Registration Reference is the same as the organization named in the organizationName field as specified in Section 7.1.4.2.2, and
- Further verify the Registration Reference matches other information verified in accordance with Section 3.2.5.

Note 2: For the following types of entities that do not have an identifier from the Registration Schemes listed in Appendix E:

- For Government Entities, the CA SHALL enter the Registration Scheme identifier 'GOV' followed by the 2 character ISO 3166 country code for the nation in which the Government Entity is located. If the Government Entity is verified at a subdivision (state or province) level, then a plus "+" (0x2B (ASCII), U+002B (UTF-8)) followed by an ISO 3166-2 identifier for the subdivision (up to three alphanumeric characters) is added.
- For International Organization Entities, the CA SHALL enter the Registration Scheme identifier 'INT' followed by the ISO 3166 code "XG". An International Organization Entity is founded by a constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments.

For example:

- GOVUS (Government Entity, United States)
- GOVUS+CA (Government Entity, United States - California)
- INTXG (International Organization)

7.1.4.2.3. S/MIME Subject DN attributes for mailbox-validated profile

Attribute	Multipurpose	Strict
commonName	MAY	MAY
organizationName	SHALL NOT	SHALL NOT
organizationalUnitName	SHALL NOT	SHALL NOT
organizationIdentifier	SHALL NOT	SHALL NOT
givenName	SHALL NOT	SHALL NOT
surname	SHALL NOT	SHALL NOT
pseudonym	SHALL NOT	SHALL NOT
serialNumber	MAY	MAY
emailAddress	MAY	MAY

Attribute	Multipurpose	Strict
title	SHALL NOT	SHALL NOT
streetAddress	SHALL NOT	SHALL NOT
localityName	SHALL NOT	SHALL NOT
stateOrProvinceName	SHALL NOT	SHALL NOT
postalCode	SHALL NOT	SHALL NOT
countryName	SHALL NOT	SHALL NOT
Other	SHALL NOT	SHALL NOT

7.1.4.2.4. S/MIME Subject DN attributes for organization-validated profile

Attribute	Multipurpose	Strict
commonName	MAY	MAY
organizationName	SHALL	SHALL
organizationalUnitName	MAY	MAY
organizationIdentifier	SHALL	SHALL
givenName	SHALL NOT	SHALL NOT
surname	SHALL NOT	SHALL NOT
pseudonym	SHALL NOT	SHALL NOT
serialNumber	MAY	MAY
emailAddress	MAY	MAY
title	SHALL NOT	SHALL NOT
streetAddress	MAY	SHALL NOT
localityName	MAY	MAY
stateOrProvinceName	MAY	MAY
postalCode	MAY	SHALL NOT
countryName	MAY	MAY
Other	SHALL NOT	SHALL NOT

7.1.4.2.5. S/MIME Subject DN attributes for sponsor-validated profile

Attribute	Multipurpose (see Note 1)	Strict (see Note 1)
commonName	MAY	MAY
organizationName	SHALL	SHALL
organizationalUnitName	MAY	MAY
organizationIdentifier	SHALL	SHALL
givenName	MAY	MAY
surname	MAY	MAY
pseudonym	MAY	MAY
serialNumber	MAY	MAY
emailAddress	MAY	MAY
title	MAY	MAY
streetAddress	MAY	SHALL NOT
localityName	MAY	MAY
stateOrProvinceName	MAY	MAY
postalCode	MAY	SHALL NOT
countryName	MAY	MAY
Other	SHALL NOT	SHALL NOT

Note 1: Multipurpose and Strict Generation profiles SHALL include either subject:givenName and/or subject:surname, or the subject:pseudonym.

7.1.4.2.6. S/MIME Subject DN attributes for individual-validated profile

Attribute	Multipurpose (see Note 1)	Strict (see Note 1)
commonName	MAY	MAY
organizationName	SHALL NOT	SHALL NOT
organizationalUnitName	SHALL NOT	SHALL NOT
organizationIdentifier	SHALL NOT	SHALL NOT
givenName	MAY	MAY
surname	MAY	MAY

Attribute	Multipurpose (see Note 1)	Strict (see Note 1)
pseudonym	MAY	MAY
serialNumber	MAY	MAY
emailAddress	MAY	MAY
title	MAY	MAY
streetAddress	MAY	SHALL NOT
localityName	MAY	MAY
stateOrProvinceName	MAY	MAY
postalCode	MAY	SHALL NOT
countryName	MAY	MAY
Other	MAY	MAY

Note 1: Multipurpose and Strict Generation profiles SHALL include either subject:givenName and/or subject:surname, or the subject:pseudonym.

7.1.4.2.7. S/MIME Subject information - root certificates and subordinate CA certificates

By issuing a Subordinate CA Certificate, the CA represents that it followed the procedure set forth in its CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

Subject distinguished name fields

Field	OID	Description
commonName	2.5.4.3	SHALL be present. This field SHOULD contain an identifier for the Certificate such that the Certificate's Name is unique across all Certificates issued by the Issuing CA.
organizationName	2.5.4.10	SHALL be present. This field SHALL contain either the Subject CA's name or DBA as verified under Section 3.2.5.2.2. 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".

Field	OID	Description
countryName	2.5.4.6	SHALL be present. This field SHALL contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.
Other attributes	-	Other attributes MAY be present within the subject field. If present, other attributes SHALL contain information that has been verified by the CA.

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.

7.1.5. S/MIME Name Constraints

For a Subordinate CA Certificate to be considered Technically Constrained, the Certificate SHALL include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue Certificates. The anyExtendedKeyUsage KeyPurposeId SHALL NOT appear within this extension.

If the Subordinate CA Certificate includes the id-kp-emailProtection extended key usage, then for the Subordinate CA Certificate to be considered Technically

Constrained it SHALL include the nameConstraints X.509v3 extension with constraints on rfc822Name and directoryName as follows:

1. For each rfc822Name in permittedSubtrees, each rfc822Name SHALL contain eithera FQDN or a U+002E FULL STOP (".") character followed by a FQDN. The rfc822Name SHALL NOT contain an email address. The CA SHALL confirm that the Applicant has registered the FQDN contained in the rfc822Name or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Section 3.2.4.3.

2. For each directoryName in permittedSubtrees, the CA SHALL confirm the Applicant's and/or Subsidiary's Organizational name and location such that end entity Certificates issued from the Subordinate CA Certificate will be in compliance with Section 7.1.2.10.

7.1.6. Certificate Policy Object Identifier

7.1.6.1. Reserved Certificate Policy Identifiers

The following policy OIDs are reserved by the CA/Browser Forum and the Apple Public CA for use by CAs as a means of asserting that a Certificate complies with the this CP.

CA/Browser Forum policy OIDs are under the *certificate-policies* arc:

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

(2.23.140.1)

{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)

The Apple Public CA policy OIDs are under these arcs:

AprCertificate arc*:*

{iso(1) member-body(2) us(840) apple(113635) appleDataSecurity(100) appleCertificatePolicies(5) applePublicPolicyID(19) AprCertificate(2)}

(1.2.840.113635.100.5.19.2)

appleISTEmailCertificatePolicyIDs arc*:*

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

(1.2.840.113635.100.5.11.5)

The table below sets forth Certificate policy OIDs available for assignment. The Apple Public CA SHALL not use the Legacy generation for S/MIME Certificate.

Certificate Type	CABF Policy OID	APR Policy OID
TLS Domain Validated	2.23.140.1.2.1	1.2.840.113635.100.5.19.2.2.1
TLS Organization Validated	2.23.140.1.2.2	1.2.840.113635.100.5.19.2.2.2
TLS Individual Validated	2.23.140.1.2.3	1.2.840.113635.100.5.19.2.2.3
SMIME Only Sign and Encrypt	-	1.2.840.113635.100.5.11.5.1
SMIME Only Sign	-	1.2.840.113635.100.5.11.5.2
SMIME Only Encrypt	-	1.2.840.113635.100.5.11.5.3
SMIME Future Use	-	1.2.840.113635.100.5.11.5.*n* where *n* may be a number between 4 and 15
Mailbox-validated - Multipurpose	2.23.140.1.5.1.2	
Mailbox-validated - Strict	2.23.140.1.5.1.3	
Organization-validated - Multipurpose	2.23.140.1.5.2.2	
Organization-validated - Strict	2.23.140.1.5.2.3	
Sponsor-validated - Multipurpose	2.23.140.1.5.3.2	
Sponsor-validated - Strict	2.23.140.1.5.3.3	
Individual-validated - Multipurpose	2.23.140.1.5.4.2	
Individual-validated - Strict	2.23.140.1.5.4.3	

7.1.6.2. S/MIME Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension. If present, the extension SHALL conform to the requirements set forth for Certificates issued to Subordinate CAs in Section 7.1.6.3.

7.1.6.3. S/MIME Subordinate CA certificates

A Certificate issued to a Subordinate CA that is not an Affiliate of the Issuing CA:

1. SHALL include one or more explicit policy identifiers defined in Section 7.1.6.1 that indicate the Subordinate CA's adherence to and compliance with this CPS and MAY contain one or more identifiers documented by the Subordinate CA in its CPS, and

2. SHALL NOT contain the anyPolicyidentifier (2.5.29.32.0).

A Certificate issued to a Subordinate CA that is an Affiliate of the Issuing CA SHALL include a set of policy identifiers from one of the two options below:

1. One or more explicit policy identifiers defined in Section 7.1.6.1 that indicate the Subordinate CA's adherence to and compliance with these Requirements and MAY contain one or more identifiers documented by the Subordinate CA in its CP and/or CPS, or
2. The anyPolicyidentifier (2.5.29.32.0).

The Subordinate CA and the Issuing CA SHALL represent, in their CPS, that all Certificates containing a policy identifier indicating compliance with these Requirements are issued and managed in accordance with this CP.

7.1.6.4. S/MIME Subscriber certificates

A Certificate issued to a Subscriber SHALL contain, within the Certificate's certificatePolicies extension, a policy identifier that is specified in Section 7.1.6.1.

The Certificate MAY also contain additional policy identifier(s) defined by the Issuing CA. The Issuing CA SHALL document in its CPS that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with this CP.

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

7.2.1. Version Number

CRLs MUST be of type X.509 v2.

7.2.2. CRL and CRL Entry Extensions

1. reasonCode (OID 2.5.29.21)
   If present, this extension MUST NOT be marked critical.

   If a CRL entry is for a Subordinate CA Certificate, including Cross-Certified Subordinate CA Certificates, this CRL entry extension MUST be present.

If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension SHOULD be present, but MAY be omitted, subject to the following requirements.

The CRLReason indicated MUST NOT be unspecified (0). If the reason for revocation is unspecified, CAs MUST omit reasonCode entry extension, if allowed by the previous requirements.

If a CRL entry is for a TLS Certificate subject to the requirements set forth in Section 1.1, the CRLReason MUST NOT be certificateHold (6).

For S/MIME, the CRLreason of certificateHold (6) SHALL NOT be used for Root CA or Subordinate CA Certificates.

The Repository MAY include CRL entries that have a CRLreason of certificateHold (6) for Certificates that include the Certificate Policy identifiers for the Multipurpose Generations. The Repository SHALL NOT include CRL entries that have a CRLreason of certificateHold (6) for Certificates that include the Certificate Policy identifiers for the Strict Generation.

If a reasonCode CRL entry extension is present, the CRLReason MUST indicate the most appropriate reason for revocation of the Certificate.

For TLS, CRLReason MUST be included in the reasonCode extension of the CRL entry corresponding to a Subscriber Certificate that is revoked after July 15, 2023, unless the CRLReason is "unspecified (0)". Revocation reason code entries for Subscriber Certificates revoked prior to July 15, 2023, do NOT need to be added or changed.

Only the following CRLReasons MAY be present in the CRL reasonCode extension for Subscriber Certificates:

- keyCompromise (RFC 5280 CRLReason #1): Indicates that it is known or suspected that the Subscriber's Private Key has been compromised;
- affiliationChanged (RFC 5280 CRLReason #3): Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised;
- superseded (RFC 5280 CRLReason #4): Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with these Baseline Requirements or the CA's CP or CPS;

- cessationOfOperation (RFC 5280 CRLReason #5): Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate; or
- privilegeWithdrawn (RFC 5280 CRLReason #9): Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

The Subscriber Agreement, or an online resource referenced therein, MUST inform Subscribers 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. Additionally, 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.

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

2. issuingDistributionPoint (OID 2.5.29.28)
   If present, this extension MUST be marked critical.

   Effective 2023-01-15, if a CRL does not contain entries for all revoked unexpired certificates issued by the CRL issuer, then it MUST contain a critical Issuing Distribution Point extension and MUST populate the distributionPoint field of that extension.

7.3. OCSP PROFILE

If an OCSP response is for a 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.

7.3.1. Version Number

No stipulation.

7.3.2. OCSP Extensions

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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CA SHALL at all times:

1. 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,
2. Comply with this CP,
3. Comply with the audit requirements set forth in this section, and
4. 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.

Note: The CAB Forum will continue to update S/MIME Baseline Requirements while CPA Canada/WebTrust and ETSI also continue to update their audit criteria. The Apple Public CA will conform to each revision of the S/MIME BRs on the date specified without waiting on a corresponding an applicable audit criterion.

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.

Period-of-time audits MUST be conducted from the time of CA Key Pair generation until the Public Key is no longer used in any 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.

If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.4, then, before issuing Publicly-Trusted Certificates, the CA SHALL successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4. The point-in-time readiness assessment SHALL be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

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. Maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

No stipulation.

8.4. TOPICS COVERED BY ASSESSMENT

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

1. "WebTrust for CAs v2.2.1 or newer" AND "WebTrust for CAs SSL Baseline with Network Security v2.5 or newer", or
2. For Audit Periods starting after September 1, 2023, "WebTrust for CAs v2.2.2 or newer" AND "WebTrust for S/MIME Baseline Requirements v1.0.0 or newer", or
3. ETSI EN 319 411-1 v1.2.2, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied).Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Auditor, as specified in 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 Issuing CA's CPS. 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).

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The APA MUST determine the significance of identified deficiencies arising from external audits or internal self-audits (Section 8.7), and MAY prescribe remediation requirements.

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 and SHALL provide it to Application Software Suppliers via the CCADB.

The CA MUST make its Audit Report available no later than three months after the end of the audit period or the point-in-time date. 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,
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, and
12. additional Audit Report requirements from Application Supplier Vendor programs.

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.

8.7. SELF-AUDITS

During the period in which the CA issues Certificates, the CA SHALL monitor adherence to this CP and its CPS 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.

8.8. REVIEW OF DELEGATED PARTIES

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 this CP and the relevant CPS.

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 this CP and the Subordinate CA's CPS. 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.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

No stipulation.

9.1.2. Certificate Access Fees

No stipulation.

9.1.3. Revocation or Status Information Access Fees

No stipulation.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. Insurance Coverage

No stipulation.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

No stipulation.

9.3.2. Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3. Responsibility To Protect Confidential Information

No stipulation.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

For TLS Certificates, no stipulation.

For S/MIME Certificates, the CA SHALL publish a Privacy Policy that provides information on the CA's data protection practices. The Privacy Policy SHOULD include information on how the CA collects, uses, shares, store, and deletes or retains data, as well as contact information for the exercise of privacy rights. The CA SHALL document where to obtain this information within Section 9.4.1 of the CA's CPS.

9.4.2. Information Treated as Private

For TLS Certificates, no stipulation.

For S/MIME Certificates, the CA or RA SHALL treat all personal information about an Individual that is not publicly available in the contents of a Certificate as private information. This includes information that links a Pseudonym to the real identity of the Subject Individual.

9.4.3. Information Not Deemed Private

No stipulation.

9.4.4. Responsibility To Protect Private Information

For TLS Certificates, no stipulation.

For S/MIME Certificates, the CA or RA SHALL protect private information using appropriate safeguards and a reasonable degree of care. The CA or RA SHALL require the same from any service providers who handle private information on behalf of the CA or RA.

9.4.5. Notice and Consent To Use Private Information

For TLS Certificates, no stipulation.

For S/MIME Certificates, the CA or RA shall provide appropriate notices to, and receive the necessary consent, from Subject Individuals before using private information for any purpose other than providing services related to the issuance and management of Certificates. The CA or RA shall require the same from any service providers who handle private information on behalf of the CA or RA.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

No stipulation.

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 this CP and its CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. Right to Use Domain Name, MailboxAddress, 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), MailboxAddress, and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names and MailboxAddresses, 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 CPS,
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 CPS,
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
    iii. accurately described the procedure in the CA's CPS,
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 7.1.4.2.2,

ii. followed the procedure when issuing the Certificate, and

iii. accurately described the procedure in the CA's CPS,

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 this CP, 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 provide information about revocation reasons and revoke the Certificate for any of the reasons specified in this CP and the Issuer CA's CPS.

The Apple Public CA, acting as the Root CA, SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with this CP, and for all liabilities and indemnification obligations of the Subordinate CA under this CP, 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:
    i. 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
    ii. 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 violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the this CP or the Issuer CA's CPS.

9.6.4. Relying Party Representations and Warranties

No stipulation.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. DISCLAIMERS OF WARRANTIES

No stipulation.

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 the CA/Browser Forum Baseline Requirements, as if the tasks had not been delegated.

If the CA has issued and managed the Certificate in compliance with the CA/Browser Forum Baseline Requirements and this CP and/or its CPS, 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 this CP and/or its CPS. If the CA has not issued or managed the Certificate in compliance with the CA/Browser Forum Baseline Requirements and this CP and/or its CPS, 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 the CA/Browser Forum Baseline Requirements or this CP and/or its CPS, then the CA SHALL include the limitations on liability in its CPS.

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 the CA/Browser Forum Baseline 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

This CP, an Issuing CA's CPS, and/or Relying Party Agreements, and any amendments thereto, SHALL become effective upon publication to the repository described in Section 2.2.

A published document SHALL remain in effect until either an updated version is published to the repository, or it is terminated in accordance with termination provision in Section 9.10.2 of this CP, or the relevant Issuing CA's CPS, or the termination provisions of the applicable agreement.

9.10.2. Termination

This CP is amended from time to time, and SHALL remain in effect until replaced by a newer version. The Issuing CA MAY set forth conditions for termination in its CPS Section 9.10.2.

9.10.3. Effect of Termination and Survival

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

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No stipulation.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

No stipulation.

9.12.2. Notification Mechanism and Period

No stipulation.

9.12.3. Circumstances Under Which OID Must Be Changed

No stipulation.

9.13. DISPUTE RESOLUTION PROVISIONS

No stipulation.

9.14. GOVERNING LAW

No stipulation.

9.15. COMPLIANCE WITH APPLICABLE LAW

No stipulation.

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.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

In the event of a conflict between the CA/Browser Forum Baseline 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 the CA/Browser Forum Baseline 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 the CA/Browser Forum Baseline Requirements accordingly.

Any modification to CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or the CA/Browser Forum Baseline Requirements 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)

No stipulation.

9.16.5. Force Majeure

No stipulation.

9.17. OTHER PROVISIONS

No stipulation.

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.

```
DNS Zone $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 visual separators.

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

```
DNS Zone $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 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.

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 Domain Name 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 Onion Domain Name using at least one of the methods listed below:
    a. The CA MAY verify the Applicant's control over the .onion service by using one of the following methods from Section 3.2.2.4:
        a. Section 3.2.2.4.18 - Agreed-Upon Change to Website v2
        b. Section 3.2.2.4.19 - Agreed-Upon Change to Website - ACME
        c. Section 3.2.2.4.20 - TLS Using ALPN

        When these methods are used to verify the Applicant's control over the .onion service, the CA MUST use Tor protocol to establish a connection to the .onion hidden service. 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 and MUST NOT issue Wildcard Certificates or use it as an Authorization Domain Name, except as specified by that method.
    b. The CA MAY verify the Applicant's control over the .onion service 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 }
            }

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 Issuing CA's CPS MAY specify a shorter validity period for Random Values.

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

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.

APPENDIX C - Definitions and Acronyms

Term	Definition
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	TLS: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates. (See Section 1.3.5.2.) S/MIME: A supplier of email client software or other relying-party application software such as mail user agents (web-based or application based) and email service providers that process S/MIME Certificates.
Assumed Name	Also known as "doing business as", "DBA", or "d/b/a" name in the US and "trading as" name in the UK.
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.

Term	Definition
Authorization Domain Name	The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "*." from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.
Authorized Ports	One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).
Base Domain Name	The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.
CAA	From RFC 8659 (http://tools.ietf.org/html/rfc8659): "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.
Certification Authority (CA)	An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs. See Section 1.3.1.
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 Management System	A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.
Certificate Policy (CP)	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement (CPS)	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Term	Definition
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Profile	A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7, e.g. a Section in a CA's CPS or a certificate template file used by CA software.
Certificate Revocation List (CRL)	A regularly updated time, stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
Certificate Systems	The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.
Certificate Transparency	A protocol for publicly logging the existence of TLS Certificates as they are issued or observed, in a manner that allows anyone to audit Certificate Authority activity and notice the issuance of suspect Certificates as well as to audit the Certificate logs themselves.
Certificate Type	The S/MIME Baseline Requirements define Certificate Profiles differentiated by the type of Subject, (for example Mailbox, Organization, Sponsored, Individual).
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%.
Conversion	The process of converting text from one writing system to ASCII characters.
Common CA Database (CCADB)	The Common CA Database is a repository of information about externally operated CAs whose Root and Subordinate Certificates are included within the products and services of Application Software Supplier that are CCADB members. Application Software Suppliers participate in the CCADB to improve security, transparency, and interoperability (See https://www.ccadb.org).
Common Vulnerability Scoring System	A quantitative model used to measure the base level severity of a vulnerability (See http://nvd.nist.gov/vuln-metrics/cvss).
Country	Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.
Critical Security Event	Detection of an event, a set of circumstances, or anomalous activity that could lead to a circumvention of a Zone's security controls or a compromise of a Certificate System's integrity, including excessive login attempts, attempts to access prohibited resources, DoS/DDoS attacks, attacker reconnaissance, excessive traffic at unusual hours, signs of unauthorized access, system intrusion, or an actual compromise of component integrity.

Term	Definition
Critical Vulnerability	A system vulnerability that has a CVSS v2.0 score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see https://nvd.nist.gov/vuln-metrics/cvss), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.
Cross-Certified Subordinate CA Certificate	A certificate that is used to establish a trust relationship between two CAs.
CSPRNG	A pseudo-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.
Delegated Third Party System	Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by the CA.
Digital Identity Document	A government-issued identity document that is issued in a machine-processable form, that is digitally signed by the issuer, and that is in purely digital form.
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 Contact	The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.
Domain Label	From RFC 8499 (http://tools.ietf.org/html/rfc8499): "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.

Term	Definition
Domain Name Registrant	Sometimes referred to as the , owner, of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the Registrant by WHOIS or the Domain Name Registrar.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: i. the Internet Corporation for Assigned Names and Numbers (ICANN), ii. a national Domain Name authority/registry, or iii. a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).
Electronic Identification (eID)	A credential containing Individual identification data and/or attributes and which is used for authentication for an online service.
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.
Extant S/MIME CA	A Subordinate CA that: i. Is a Publicly-Trusted Subordinate CA Certificate whose `notBeforefield` is before September 1, 2023 and has issued end entity S/MIME Certificates, ii. The CA Certificate includes no Extended Key Usage extension, contains `anyExtendedKeyUsage` in the EKU extension, or contains `id-kp-emailProtection` in the EKU extension, iii. The CA Certificate complies with the profile defined in RFC 5280 (http://tools.ietf.org/html/rfc5280). The following two deviations from the RFC 5280 profile are acceptable: a. The CA Certificate contains a `nameConstraints` extension that is not marked critical, b. The CA Certificate contains a policy qualifier of type `UserNotice` which contains `explicitText` that uses an encoding that is not permitted by RFC 5280 (i.e., the `DisplayText` is encoded using BMPString or VisibleString), and iv. The CA Certificate contains the `anyPolicyidentifier` (2.5.29.32.0) or specific OIDs in the `certificatePolicies` extension that do not include those defined in Section 7.1.6.1.
Front End / Internal Support System	A system with a public IP address, including a web server, mail server, DNS server, jump host, or authentication server.
Fully-Qualified Domain Name (FQDN)	A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.
Generation	The S/MIME Baseline Requirements define several Generations of Certificate Profile for each Certificate Type.

Term	Definition
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.
High Security Zone	A physical location where a CA's or Delegated Third Party's Private Key or cryptographic hardware is located.
Incident	A CA's failure to comply with any requirement of this CP - whether it be a misissuance, a procedural or operational issue, or any other variety of non-compliance.
Individual	A Natural Person.
Individual-Validated	Refers to an S/MIME Certificate Subject that includes only Individual (Natural Person) attributes, rather than attributes linked to an Organization.
Internal Name	A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.
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).
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.
Issuing System	A system used to sign certificates or validity status information.
Jurisdiction of Incorporation	The country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.
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.

Term	Definition
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 (http://tools.ietf.org/html/rfc5890): "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."
Legacy Profile	The S/MIME Legacy Generation profiles provide flexibility for existing reasonable S/MIME certificate practices to become auditable under the S/MIME Baseline Requirements. This includes options for Subject DN attributes, `extKeyUsage`, and other extensions. The Legacy Profiles will be deprecated in a future version of the S/MIME Baseline Requirements.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Multi-Factor Authentication	An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction: something you know (knowledge factor), something you have (possession factor), and something you are (inherence factor). Each factor must be independent. Certificate-based authentication can be used as part of Multifactor Authentication only if the private key is stored in a Secure Key Storage Device.
Mailbox-Validated (MV)	Refers to a Certificate Subject that is limited to (optional) `subject:emailAddress` or `subject:commonName`, and/or `subject:serialNumber` attributes.
Mailbox Address	Also Email Address. The format of a Mailbox Address is defined as a "Mailbox" as specified in Section 4.1.2 of RFC 5321 (http://tools.ietf.org/html/rfc5321) and amended by Section 3.2 of RFC 6532 (http://tools.ietf.org/html/rfc6532), with no additional padding or structure.
Mailbox Field	In Subscriber Certificates contains a Mailbox Address of the Subject via `rfc822Name` or `otherName` value of type `id-on-SmtpUTF8Mailbox` in the `subjectAltName` extension, or in Subordinate CA Certificates via `rfc822Name` in permittedSubtrees within the nameConstraints extension.
Multipurpose Profile	The S/MIME Multipurpose Generation profiles are aligned with the more defined Strict Profiles, but with additional options for `extKeyUsage` and other extensions. This is intended to allow flexibility for crossover use cases between document signing and secure email.
National Vulnerability Database	A database that includes the Common Vulnerability Scoring System (CVSS) scores of security-related software flaws, misconfigurations, and vulnerabilities associated with systems (see http://nvd.nist.gov/).
Natural Person	An Individual; a human being as distinguished from a Legal Entity.
Non-Reserved LDH Label (NR-LDH)	From RFC 5890 (http://tools.ietf.org/html/rfc5890): "The set of valid LDH labels that do not have '–' in the third and fourth positions."

Term	Definition
Object Identifier (OID)	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.
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 (OCSP)	An online Certificate, checking protocol that enables relying, party application software to determine the status of an identified Certificate. See also OCSP Responder.
Organization-Validated	Refers to a Certificate Subject that includes only Organizational (Legal Entity) attributes, rather than attributes linked to an Individual.
OWASP Top Ten	A list of application vulnerabilities published by the Open Web Application Security Project (see https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).
P-Label	A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.
Parent Company	A company that Controls a Subsidiary Company.
Personal Name	Personal Name is a name of an Individual Subject typically presented as `subject:givenName` and/or `subject:surname`. However, the Personal Name may be in a format preferred by the Subject, the CA, or Enterprise RA as long as it remains a meaningful representation of the Subject's verified name.
Physical Identity Document	A government-issued identity document issued in physical and human-readable form (such as a passport or national identity card)
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.
Penetration Test	A process that identifies and attempts to exploit openings and vulnerabilities on systems through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.

Term	Definition
Precertificate	A cryptographic object that is constructed from the Certificate to be issued by adding a special critical poison extension (OID 1.3.6.1.4.1.11129.2.4.3, and extnValue NULL) to the end-entity TBSCertificate and signing the resulting TBSCertificate [RFC5280] with either: • a special-purpose (CA:true, Extended Key Usage: Certificate Transparency, OID 1.3.6.1.4.1.11129.2.4.4) Precertificate signing certificate. The Precertificate signing certificate MUST be directly certified by the (Root CA or Subordinate CA) Certificate that will ultimately sign the end-entity TBSCertificate yielding the end-entity Certificate, or, • the Subordinate CA Certificate that will sign the final certificate.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Pseudonym	A fictitious identity that a person assumes for a particular purpose. Unlike an anonymous identity, a pseudonym can be linked to the person's real identity.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Public Key Infrastructure (PKI)	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 CA Certificate is distributed as a trust anchor in widely, available application software.
Qualified Auditor	A natural person or Legal Entity that meets the requirements of 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. See Section 1.3.2.
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.

Term	Definition
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. Section 1.3.4.
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. 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: 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f 7c5f26cf14f
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 collection of Baseline Requirements and Application Software Suppliers program requirements listed in Section 1.1.

Term	Definition
Reserved IP Address	An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries: https://www.iana.org/assignments/iana-ipv4-special-registry/ iana-ipv4-special-registry.xhtml https://www.iana.org/assignments/iana-ipv6-special-registry/ iana-ipv6-special-registry.xhtml
Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
Root CA System	A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.
Root CA Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
S/MIME	Secure/Multipurpose Internet Mail Extensions (S/MIME) is a widely accepted standard for sending digitally signed and encrypted messages. See RFC5751 for further details.
S/MIME Certificate	A Certificate with an Extended Key Usage extension populated with the value id-kp-emailProtection [RFC5280], and that is not Root Certificate or Subordinate CA certificate.
SANS Top 25	A list created with input from the SANS Institute and the Common Weakness Enumeration (CWE) that identifies the Top 25 Most Dangerous Software Errors that lead to exploitable vulnerabilities (see http://www.sans.org/top25-software-errors/).
Secure Key Storage Device	A device certified as meeting at least FIPS 140-2 level 2 overall, level 3 physical, or Common Criteria (EAL 4+).
Secure Zone	An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems.
Security Support System	A system used to provide security support functions, which MAY include authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and intrusion detection (Host-based intrusion detection, Network-based intrusion detection).
Sovereign State	A state or country that administers its own government, and is not dependent upon, or subject to, another power.
Sponsor-validated	Refers to a Certificate Subject which combines Individual (Natural Person) attributes in conjunction with an `subject:organizationName` (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA where the `subject:organizationName` is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent
Strict Profile	The S/MIME Strict Generation profiles are the long term target profile for S/MIME Certificates with `extKeyUsage` limited to `id-kp-emailProtection`, and stricter use of Subject DN attributes and other extensions.

Term	Definition
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 or mailbox under the control and operation of the Subscriber.
Subject Identity Information	Information that identifies the Certificate Subject. TLS: Subject Identity Information does not include a Domain Name listed in the `subjectAltName` extension or the Subject `commonName` field. S/MIME: Subject Identity Information does not include a Mailbox Address listed in the `subject:commonName` or `subject:emailAddress` fields, or in the `subjectAltName` extension.
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. See Section 1.3.3.
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.
Supplementary Evidence	Used in addition to authoritative evidence to strengthen the reliability of the identity verification and/or as evidence for attributes that are not evidenced by the authoritative evidence.
System	One or more pieces of equipment or software that stores, transforms, or communicates data.
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.
TLS Certificate	A Certificate with an Extended Key Usage extension populated with either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values, and that is not Root Certificate or Subordinate CA certificate.
Trusted Role	An employee or contractor of a CA or Delegated Third Party who has authorized access to or control over a Secure Zone or High Security Zone.
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.

Term	Definition
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialists	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."
Vulnerability Scan	A process that uses manual or automated tools to probe internal and external systems to check and report on the status of operating systems, services, and devices exposed to the network and the presence of vulnerabilities listed in the NVD, OWASP Top Ten, or SANS Top 25.
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 (http://tools.ietf.org/html/rfc5890): "The class of labels that begin with the prefix "xn--" (case independent), but otherwise conform to the rules for LDH labels."
Zone	A subset of Certificate Systems created by the logical or physical partitioning of systems from other Certificate Systems.

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

Acronym	Term
AICPA	American Institute of Certified Public Accountants
ADN	Authorization Domain Name
APA	Apple Policy Authority
CA	Certification Authority
CAA	Certification Authority Authorization
CAMT	Certification Authority Management Team
CCADB	Common Certification Authority Database
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CVSS	Common Vulnerability Scoring System
CT	Certificate Transparency
DBA	Doing Business As
DNS	Domain Name System
DN	Distinguished Name
ETSI	European Telecommunications Standards Institute
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
ICAO	International Civil Aviation Organization
ISO	International Organization for Standardization
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HSE	High Security Environment

Acronym	Term
MV	Mailbox-validated
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NVD	National Vulnerability Database
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure/Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VoIP	Voice Over Internet Protocol

APPENDIX D - Network and Certificate System Security Requirements

For the requirements in this Appendix, the CA is responsible for all tasks performed by Delegated Third Parties and Trusted Roles, and the CA SHALL define, document, and disclose to its auditors

1. the tasks assigned to Delegated Third Parties or Trusted Roles, and
2. the arrangements made with Delegated Third parties to ensure compliance with these requirements, and
3. the relevant practices implemented by Delegated Third Parties.

1. GENERAL PROTECTIONS FOR THE NETWORK AND SUPPORTING SYSTEMS

Each CA or Delegated Third Party SHALL:

1. Segment Certificate Systems into networks based on their functional or logical relationship, for example separate physical networks or VLANs,
2. Apply equivalent security controls to all systems co-located in the same network with a Certificate System,
3. Maintain Root CA Systems in a High Security Zone and in an offline state or air-gapped from all other networks,
4. Maintain and protect Issuing Systems, Certificate Management Systems, and Security Support Systems in at least a Secure Zone,
5. Implement and configure Security Support Systems that protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks,
6. 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 that the CA has identified as necessary to its operations,
7. Configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party,
8. Ensure that the CA's security policies encompass a change management process, following the principles of documentation, approval and review, and to ensure that all changes to Certificate Systems, Issuing Systems, Certificate Management Systems,

Security Support Systems, and Front-End / Internal-Support Systems follow said change management process,

9. Grant administration access to Certificate Systems only to persons acting in Trusted Roles and require their accountability for the Certificate System's security,
10. Implement Multi-Factor Authentication to each component of the Certificate System that supports Multi-Factor Authentication,
11. Change authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked, and
12. Apply recommended security patches to Certificate Systems 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.

2. TRUSTED ROLES, DELEGATED THIRD PARTIES, AND SYSTEM ACCOUNTS

Each CA or Delegated Third Party SHALL:

1. Follow a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them,
2. Document the responsibilities and tasks assigned to Trusted Roles and implement "separation of duties" for such Trusted Roles based on the security-related concerns of the functions to be performed,
3. Ensure that only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones,
4. Ensure that an individual in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role,
5. Require employees and contractors to observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems,
6. Require that each individual in a Trusted Role use a unique credential created by or assigned to that person in order to authenticate to Certificate Systems (for accountability purposes, group accounts or shared role credentials SHALL NOT be used),
7. If an authentication control used by a Trusted Role is a username and password, then, where technically feasible, implement the following controls:
    a. For accounts that are accessible only within Secure Zones or High Security Zones, require that passwords have at least twelve (12) characters,
    b. For authentications which cross a zone boundary into a Secure Zone or High Security Zone, require Multi-Factor Authentication. For accounts accessible from

outside a Secure Zone or High Security Zone require passwords that have at least eight (8) characters and are not be one of the user's previous four (4) passwords; and implement account lockout for failed access attempts in accordance with subsection 11 below,

c. When developing password policies, CAs SHOULD take into account the password guidance in NIST 800-63B Appendix A.

d. Frequent password changes have been shown to cause users to select less secure passwords. If the CA has any policy that specifies routine periodic password changes, that period SHALL NOT be less than two years.

8. Have a policy that requires Trusted Roles to log out of or lock workstations when no longer in use,
9. Have a procedure to configure workstations with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user (the CA or Delegated Third Party MAY allow a workstation to remain active and unattended if the workstation is otherwise secured and running administrative tasks that would be interrupted by an inactivity time-out or system lock),
10. Review all system accounts at least every three (3) months and deactivate any accounts that are no longer necessary for operations,
11. Lockout account access to Certificate Systems after no more than five (5) failed access attempts, provided that this security measure,
    a. Is supported by the Certificate System,
    b. Cannot be leveraged for a denial of service attack, and
    c. Does not weaken the security of this authentication control,
12. Implement a process that disables all privileged access of an individual to Certificate Systems within twenty four (24) hours upon termination of the individual's employment or contracting relationship with the CA or Delegated Third Party,
13. Enforce Multi-Factor Authentication OR multi-party authentication for administrator access to Issuing Systems and Certificate Management Systems,
14. Enforce Multi-Factor Authentication for all Trusted Role accounts on Certificate Systems (including those approving the issuance of a Certificate, which equally applies to Delegated Third Parties) that are accessible from outside a Secure Zone or High Security Zone, and
15. Restrict remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when:
    a. the remote connection originates from a device owned or controlled by the CA or Delegated Third Party,
    b. the remote connection is through a temporary, non-persistent encrypted channel that is supported by Multi-Factor Authentication, and
    c. the remote connection is made to a designated intermediary device
        i. located within the CA's network,

ii. secured in accordance with these Requirements, and

iii. that mediates the remote connection to the Issuing System.

3. LOGGING, MONITORING, AND ALERTING

Certification Authorities and Delegated Third Parties SHALL:

1. Implement a System under the control of CA or Delegated Third Party Trusted Roles that continuously monitors, detects, and alerts personnel to any modification to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems unless the modification has been authorized through a change management process. The CA or Delegated Third Party shall respond to the alert and initiate a plan of action within at most twenty-four (24) hours,
2. Identify those Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity, and enable those systems to log and continuously monitor the events specified in Section 5.4.1 (3) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,
3. Implement automated mechanisms under the control of CA or Delegated Third Party Trusted Roles to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events,
4. Require Trusted Role personnel to follow up on alerts of possible Critical Security Events,
5. Monitor the integrity of the logging processes for application and system logs through continuous automated monitoring and alerting or through a human review to ensure that logging and log-integrity functions are effective. Alternatively, if a human review is utilized and the system is online, the process must be performed at least once every 31 days.
6. Monitor the archival and retention of logs to ensure that logs are retained for the appropriate amount of time in accordance with the disclosed business practices and applicable legislation.
7. If continuous automated monitoring and alerting is utilized to satisfy Sections 1.8. or 3.4. of this Appendix D, respond to the alert and initiate a plan of action within at most twenty-four (24) hours.

4. VULNERABILITY DETECTION AND PATCH MANAGEMENT

Certification Authorities and Delegated Third Parties SHALL:

1. Implement intrusion detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles to protect Certificate Systems against common network and system threats,

2. Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities,
3. Undergo or perform a Vulnerability Scan
    a. within one (1) week of receiving a request from the CA/Browser Forum,
    b. after any system or network changes that the CA determines are significant, and
    c. at least every three (3) months, on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems,
4. Undergo a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant,
5. Record evidence that each Vulnerability Scan and Penetration Test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test, and
6. Do one of the following within ninety-six (96) hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process:
    a. Remediate the Critical Vulnerability,
    b. If remediation of the Critical Vulnerability within ninety-six (96) hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to
        i. vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0) and
        ii. systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise, or
    c. Document the factual basis for the CA's determination that the vulnerability does not require remediation because
        i. the CA disagrees with the NVD rating,
        ii. the identification is a false positive,
        iii. the exploit of the vulnerability is prevented by compensating controls or an absence of threats, or
        iv. other similar reasons.

APPENDIX E – Registration schemes

E.1. ORGANIZATIONIDENTIFIER

The following Registration Schemes are recognized as valid under these Requirements for use in the subject:organizationIdentifier attribute described in Section 7.1.4.2.2.

The country code used in the Registration Scheme identifier SHALL match that of the subject:countryName in the Certificate as specified in Section 7.1.4.2.2.

- **NTR**: For an identifier allocated by a national or state trade register to the Legal Entity named in the subject:organizationName.
- **VAT**: For an identifier allocated by the national tax authorities to the Legal Entity named in the subject:organizationName.
- **PSD**: For a national authorization number allocated to the payment service provider named in the subject:organizationName under Payments Services Directive (EU) 2015/2366. This shall use the extended structure as defined in ETSI TS 119 495, clause 5.2.1.
- **LEI**: For a Legal Entity Identifier as specified in ISO 17442 for the entity named in the subject:organizationName. The 2 character ISO 3166 country code SHALL be set to 'XG'.

E.2. NATURAL PERSON IDENTIFIER

The following Registration Schemes are recognized as valid for use in the subject:serialNumber attribute described in Section 7.1.4.2.2.

- **PAS**: For an identifier based on a passport number issued to the Subject Individual.
- **IDC**: For an identifier based on a national identity card issued to the Subject Individual.
- **PNO**: For an identifier based on a national personal number (or national civic registration number) issued to the Subject Individual.
- **TIN**: For an identifier based on Tax Identification Number issued to the Subject Individual.

APPENDIX F – Transition of Extant S/MIME CAs

Following the Effective Date for v 1.0.0 of these Requirements (September 1, 2023) an Extant S/MIME CA MAY continue to issue end entity S/MIME Certificates that are compliant with these Requirements.

On or after September 15, 2024, all newly-issued Publicly-Trusted end entity S/MIME Certificates SHALL be issued from S/MIME Subordinate CAs that are compliant with these Requirements.

For backwards compatibility, Extant S/MIME CA Certificates that share the same Public Keys with S/MIME Subordinate CAs that are compliant with these Requirements, or are no longer used for signing end entity S/MIME Certificates, are not required to be revoked.