Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates

Version 1.0.14

May 5, 2026

Table of Contents

1. INTRODUCTION

1.1 Overview

This S/MIME Baseline Requirements document 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 S/MIME Certificates.

An S/MIME Certificate for the purposes of this document can be identified by the existence of an Extended Key Usage (EKU) for `id-kp-emailProtection` (OID: 1.3.6.1.5.5.7.3.4) and the inclusion of a `rfc822Name` or an `otherName` of type `id-on-SmtpUTF8Mailbox` in the `subjectAltName` extension.

Notice for Readers

An S/MIME Certificate contains a Public Key bound to a Mailbox Address and MAY also contain the identity of a Natural Person or Legal Entity that controls such email address. The Key Pair can then be used to sign, verify, encrypt, and decrypt email.

This Certificate Policy (CP) describes a subset of the requirements that a CA SHALL meet in order to issue Publicly-Trusted S/MIME Certificates. This document serves two purposes: to specify Baseline Requirements and to provide guidance and requirements for what a Certification Authority (CA) should include in its Certification Practice Statement (CPS). These Requirements apply only to relevant events that occur on or after the relevant Effective Date described in Section 1.2.1 of these Requirements.

These Requirements do not address all of the issues relevant to the issuance and management of Publicly-Trusted S/MIME Certificates. To facilitate a comparison of other CP and/or CPS (e.g., for policy mapping), this document includes all sections of the RFC 3647 framework. The CA/Browser Forum MAY update these Requirements from time to time.

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

These Requirements are applicable to all CAs within a Publicly-Trusted chain of trust. They are to be flowed down from the Root CA through successive Subordinate CAs.

1.2 Document name and identification

This Certificate Policy contains the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, as adopted by the CA/Browser Forum.

These Requirements describe four Certificate profiles differentiated by the type of Subject:

Certificate Type	Description
Mailbox-validated	Subject is limited to (optional) `subject:emailAddress`, `subject:commonName`, and/or `subject:serialNumber` attributes.
Organization-validated	Includes only Organizational (Legal Entity) attributes in the Subject.
Sponsor-validated	Combines Individual (Natural Person) attributes in conjunction with a `subject:organizationName` (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA.
Individual-validated	Includes only Individual (Natural Person) attributes in the Subject.

In addition, Generations (known as Legacy, Multipurpose, and Strict) are specified for each of these Certificate Types, acknowledging both the current diversity of practice in issuing S/MIME Certificates as well as the desire to move towards more closely-defined practices over time.

The following Certificate Policy identifiers are reserved for use by CAs as a means of asserting compliance with this document (OID arc 2.23.140.1.5) as follows:

Mailbox-validated
`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) legacy (1)}` (2.23.140.1.5.1.1); and

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) multipurpose (2)}` (2.23.140.1.5.1.2); and

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) strict (3)}` (2.23.140.1.5.1.3); and

Organization-validated
`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) legacy (1)}` (2.23.140.1.5.2.1); and

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) multipurpose (2)}` (2.23.140.1.5.2.2); and

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) strict (3)}` (2.23.140.1.5.2.3); and

Sponsor-validated
`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) legacy (1)}` (2.23.140.1.5.3.1); and

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) multipurpose (2)}` (2.23.140.1.5.3.2); and

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) strict (3)}` (2.23.140.1.5.3.3); and

Individual-validated
`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) legacy (1)}` (2.23.140.1.5.4.1); and

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) multipurpose (2)}` (2.23.140.1.5.4.2); and

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) strict (3)} (2.23.140.1.5.4.3).

1.2.1 Revisions

Version	Ballot	Description	Publication Date*
1.0.0	SMC01	Version 1.0 of the S/MIME Baseline Requirements adopted	January 01, 2023
1.0.1	SMC03	Clarification and corrections	August 11, 2023
1.0.2	SMC04	Addition of ETSI TS 119 411-6	December 8, 2023
1.0.3	SMC05	Introduction of CAA for S/MIME	February 20, 2024
1.0.4	SMC06	Post implementation clarification and corrections	May 11, 2024
1.0.5	SMC07	Align Logging Requirement and Key Escrow clarification	July 15, 2024
1.0.6	SMC08	Deprecate Legacy Generation Profiles and Minor Updates	August 29, 2024
1.0.7	SMC09	Update to WebTrust requirements, require linting, minor edits	November 22, 2024
1.0.8	SMC010	Introduction of Multi-Perspective Issuance Corroboration	December 22, 2024
1.0.9	SMC011	Add EUID as Registration Reference	May 14, 2025
1.0.10	SMC012	ACME for S/MIME Automation	July 2, 2025
1.0.11	SMC013	Introduction of PQC Algorithms	August 22, 2025
1.0.12	SMC014	DNSSEC for CAA	October 13, 2025
1.0.13	SMC015	Allow mDL for Authentication of Individual Identity	March 27, 2026
1.0.14	SMC016	Equivalence with Ballots SC096 and SC097	May 5, 2026

* Publication Date is the date the new version was published following the Intellectual Property Review.

Version	Ballot	Description	Additional Compliance Date
1.0.0	SMC01	Initial implementation date	September 01, 2023
1.0.1	SMC03	Transition end for Extant S/MIME CAs	September 15, 2024
1.0.3	SMC05	SHOULD adoption of CAA for S/MIME	September 15, 2024
1.0.3	SMC05	SHALL adoption of CAA for S/MIME	March 15, 2025
1.0.4	SMC06	Requirement to check Active status of Legal Entity Applicants	September 15, 2024
1.0.6	SMC08	S/MIME Subscriber Certificates SHALL NOT be issued using the Legacy Generation profiles	July 15, 2025
1.0.7	SMC09	WebTrust audits SHALL include WebTrust for Network Security	April 1, 2025
1.0.7	SMC09	SHOULD implement pre-issuance linting of S/MIME Certificates, and SHOULD implement use of Linting in Self-Audits	March 15, 2025
1.0.7	SMC09	SHALL implement pre-issuance linting of S/MIME Certificates	September 15, 2025
1.0.8	SMC010	SHOULD implement MPIC	March 15, 2025
1.0.8	SMC010	SHALL implement MPIC	May 15, 2025
1.0.12	SMC014	SHALL implement DNSSEC for CAA	March 15, 2026
1.0.14	SMC016	SHALL sunset all remaining use of SHA-1 in Certificates and CRLs	September 15, 2026

1.3 PKI participants

The CA/Browser Forum is a voluntary organization of Certification Authorities and Application Software Suppliers including providers of Internet browser and other relying-party software applications, such as mail user agents (web-based or application-based) and email service providers that process S/MIME Certificates.

1.3.1 Certification authorities

Certification Authority (CA) is defined in Section 1.6.1. Current CA Members of the CA/Browser Forum are listed at https://cabforum.org/members.

1.3.2 Registration authorities

With the exception of Section 3.2.2, the CA MAY delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 3.2.

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

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

1.3.2.1 Enterprise registration authorities

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 3.2.2.1 or Section 3.2.2.3.
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 3.2.2.2 or Section 3.2.2.4.

1.3.3 Subscribers

As defined in Section 1.6.1.

1.3.4 Relying parties

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

1.3.5 Other participants

Other groups that have participated in the development of these Requirements include the CPA Canada WebTrust for Certification Authorities task force and the Accredited Conformity Assessment Bodies’Council (ACAB’C). Participation by these groups does not imply their endorsement, recommendation, or approval of the final product.

1.4 Certificate usage

The primary goal of these Requirements 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.

1.4.1 Appropriate certificate uses

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.

1.4.2 Prohibited certificate uses

No stipulation.

1.5 Policy administration

These Requirements MAY be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. The CA/Browser Forum welcomes recommendations and suggestions regarding this standard by email at questions@cabforum.org.

1.5.1 Organization administering the document

No stipulation.

1.5.2 Contact person

Contact information for the CA/Browser Forum is available at https://cabforum.org/leadership/. In this section of a CA’s CPS, the CA SHALL provide a link to a web page or an email address for contacting the person or persons responsible for operation of the CA, including contact information for entities wishing to submit a Certificate Problem Report or revocation request.

1.5.3 Person determining CPS suitability for the policy

No stipulation.

1.5.4 CPS approval procedures

No stipulation.

1.6 Definitions and acronyms

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

1.6.1 Definitions

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

Applicant: The Natural Person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, 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:

1. who signs and submits, or approves a Certificate Request on behalf of the Applicant;
2. who signs and submits a Subscriber Agreement on behalf of the Applicant; and/or
3. who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of 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: 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.

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

Certification Authority Authorization (or CAA): From RFC 9495: "The Certification Authority Authorization (CAA) DNS resource record (RR) provides a mechanism for domains to express the allowed set of Certification Authorities that are authorized to issue certificates for the domain."

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

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

Certificate Policy (or 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 (or CPS): One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

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

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.

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

Cross Certificate: A Certificate that is used to establish a trust relationship between two Root 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.

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.

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

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

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.

European Unique Identifier (EUID): The EUID uniquely identifies officially-registered organizations, Legal Entities, and branch offices within the European Union or the European Economic Area. The EUID is specified in chapter 9 of the Annex contained in the Implementing Regulation (EU) 2021/1042 which describes rules for the application of Directive (EU) 2017/1132 "relating to certain aspects of company law (codification)".

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:

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

Fully-Qualified Domain Name: 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.

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.).

Individual: A Natural Person.

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

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.

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.

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.

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.

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

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

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

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

Mobile Driver License (mDL): A driver license that is issued in digital format by an Issuing Authority that is authorized by the relevant government or jurisdiction to issue driving licenses in accordance with applicable law, and conforms to ISO/IEC 18013-5 and ISO/IEC 18013-7.

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

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

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

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

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

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

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

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

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).

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

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

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

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

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root 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. An RA MAY assist in the certificate application process or revocation process or both. When "RA"is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Registration Reference: An identifier assigned to a Legal Entity.

Registration Scheme: A scheme for assigning a Registration Reference meeting the requirements identified in Appendix A.

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

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

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

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Requirements: The S/MIME Baseline Requirements found in this document.

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

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.

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 of the named Subject Organization.

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.

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 mailbox under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. 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.

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.

Technically Constrained Subordinate CA Certificate: A Subordinate CA Certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate MAY issue Certificates to Subscriber or additional Subordinate CAs.

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.

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

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

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

1.6.2 Acronyms

Acronym	Meaning
CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
ETSI	European Telecommunications Standards Institute
FIPS	(US Government) Federal Information Processing Standard
ICAO	International Civil Aviation Organization
ISO	International Organization for Standardization
mDL	Mobile Driver License
MPIC	Multi-perspective issuance corroboration
MV	Mailbox-validated

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

1.6.3 References

eIDAS: Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183 and Directive (EU) 2022/2555

ETSI EN 319 403-1, Electronic Signatures and Trust 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 Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

ETSI EN 319 411-2, Electronic Signatures and Trust 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 119 411-6, Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates.

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

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

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

ETSI TS 119 495, Electronic Signatures and Trust 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.

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/IEC TS 18013-5, Information technology —Personal identification —ISO-compliant driving licence —Part 5: Mobile Driving Licence (mDL) application.

ISO/IEC TS 18013-7, Information technology —Personal identification —ISO-compliant driving licence —Part 7: Mobile Driving Licence (mDL) digital trust service.

Network and Certificate System Security Requirements, Version 2.0 or later. See https://cabforum.org/network-security-requirements/.

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications.

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

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

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

RFC4035, Request for Comments: 4035, Protocol Modifications for the DNS Security Extensions. R. Arends, et al. March 2005.

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

RFC4509, Request for Comments: 4509, Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs). W. Hardaker. May 2006.

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

RFC5155, Request for Comments: 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. B. Laurie, et al. March 2008.

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

RFC5702, Request for Comments: 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC. J. Jansen. October 2009.

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

RFC6840, Request for Comments: 6840, Clarifications and Implementation Notes for DNS Security (DNSSEC). S. Weiler, et al. February 2013.

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

RFC 8823, Request for Comments: 8823, Extensions to Automatic Certificate Management Environment for End-User S/MIME Certificates, A. Melnikov. April 2021.

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

RFC 9598, Request for Comments: 9598, Internationalized Email Addresses in X.509 Certificates, A. Melnikov, et al. May 2024.

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

RFC 9495, Request for Comments: 9495, Certification Authority Authorization (CAA) Processing for Email Addresses, C. Bonnell. October 2023.

RFC 9598, Request for Comments: 9598, Internationalized Email Addresses in X.509 Certificates, A. Melnikov, et al. May 2024.

“TLS Baseline Requirements”means the current 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/

WebTrust for Certification Authorities, CPA Canada.

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

1.6.4 Conventions

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

2.2 Publication of certification information

The CA SHALL publicly disclose its CP and/or CPS through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see Section 8).

The CP and/or CPS SHALL be structured in accordance with RFC 3647 and SHALL include all material required by RFC 3647.

The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version. The CA MAY fulfill this requirement by incorporating these Requirements directly into its 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 Certificate Policy and/or Certification Practice Statement (CP and/or CPS) that describes in detail how the CA implements the latest version of these Requirements. The CA SHALL review and update its CP and/or CPS at least every 365 days, incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

2.4 Access controls on repositories

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

No stipulation.

3.1.1 Types of names

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(a).

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

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

3.1.2 Need for names to be meaningful

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

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 CP and/or 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 3.2.4. 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 3.2.4. 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 for interpreting various name forms

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

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 Mailbox Addresses to be included in the S/MIME Certificate according to the requirements of the following sections:

Certificate Type	Mailbox Control	Organization Identity	Individual Identity
`Mailbox-validated`	Section 3.2.2	NA	NA
`Organization-validated`	Section 3.2.2	Section 3.2.3	NA
`Sponsor-validated`	Section 3.2.2	Section 3.2.3	Section 3.2.4
`Individual-validated`	Section 3.2.2	NA	Section 3.2.4

3.2.1 Method to prove possession of private key

No stipulation.

3.2.2 Validation of mailbox authorization or control

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

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.

3.2.2.1 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 of the TLS Baseline Requirements to perform this verification.

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

3.2.2.2 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.

3.2.2.3 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 of the TLS Baseline Requirements.

3.2.2.4 Validating control over mailbox using ACME extensions

The CA MAY confirm the Applicant's control over each Mailbox Field to be included in a Certificate using ACME for S/MIME as defined in RFC 8823. The CA's ACME server MAY respond to a POST request by sending the Random Value token components via email and SMTP, and then receiving a confirming response utilizing the generated Random Value, in accordance with RFC 8823.

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

The Random Value SHALL NOT be reused by the CA for other Certificate Requests. The Random Value SHALL remain valid for use in a confirming response for no more than 24 hours from its creation. The CA MAY specify a shorter validity period for Random Values in its CP and/or CPS.

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

3.2.3 Authentication of organization identity

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

3.2.3.1 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 Affiliate of the Legal Entity as described in Section 7.1.4.2.2 (if included in the Subject as an `subject:organizationalUnitName`);
4. An address of the Legal Entity (if included in the Subject);
5. Jurisdiction of Incorporation or Registration of the Legal Entity; and
6. Identifier and type of identifier for the Legal Entity.

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

3.2.3.2 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 3.2.8.

3.2.3.2.1 Verification of name, address, and 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) and its current status.

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.

In cases 1 and 4 above, the CA or RA SHALL verify that the status of the Applicant is not designated by labels such as "ceased,""inactive,""invalid,""not current,"or the equivalent.

In case 2 above when 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.

3.2.3.2.2 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.

3.2.3.3 Disclosure of verification sources

The CA or RA SHALL verify the Registration Reference to be included 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.

3.2.4 Authentication of individual identity

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

The CA, RA, or Enterprise 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 or 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.

3.2.4.1 Attribute collection of individual identity

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

1. **From a physical identity document**

If physical identity documents are used to provide 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.

2. **From a digital identity document**

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

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

3. **Using electronic identification schemes (eID)**

If an eID is used to provide 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.

4. **From a certificate supporting a digital signature applied by the Applicant**

If a digital signature is used to provide 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.

a. Approved Frameworks

- To be added by subsequent ballot.

b. Criteria to propose additional frameworks

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.

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.

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 3.2.8.

The CA or RA SHALL still verify the identity of the Individual in accordance with Section 3.2.4 and the Organization in accordance with Section 3.2.3.

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.

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, an eligible eID, an eligible mDL, 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.

9. **From a Mobile Driver License (mDL)**

If an mDL is used to provide evidence, the CA or RA SHALL only accept an mDL that:

- Is issued by an Issuing Authority that is legally authorized by the relevant government or jurisdiction to issue driving licenses;
- Conforms to ISO/IEC 18013-5;
- Supports validation through the verification protocols defined in ISO/IEC 18013-7; and
- Can demonstrate a valid Certificate chain from the Document Signer Certificate to an Issuing Authority Certificate that is verifiable through a publicly available trust anchor or trust list approved by the issuing jurisdiction.

The CA SHALL document and publish information describing the issung jurisdictions and mDL versions it accepts.

3.2.4.2 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.

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).

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 against the relevant country signing Certificates (e.g., from the ICAO Public Key Database).

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. **Validation of eID**

If authentication using an eID is used to provide 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.

4. **Validation of digital signature with certificate**

If a digital signature with Certificate is used to provide 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.

5. **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.

6. **Validation of affiliation from a company attestation**

The reliability of the Attestation SHALL be verified according to Section 3.2.8.

7. **Validation of a general attestation**

The reliability of the Attestation SHALL be verified according to Section 3.2.8.

8. **Validation of a supplementary evidence**

No stipulation.

9. **Validation of an mDL**

If an mDL is used to provide evidence, the CA or RA SHALL:

- Authenticate to the mDL holder's device and request data in conformance with ISO/IEC 18013-5 and ISO/IEC 18013-7;
- Verify the authenticity and integrity of the mDL data through validation of the Mobile Security Object (MSO) and its signature chain;
- Validate the Document Signer Certificate chain against the issuing jurisdiction's published trust infrastructure; and
- Verify that the mDL is current and has not been revoked or expired.

The mDL authentication SHALL be performed in real-time as part of the identity validation process, and SHALL NOT rely on previously captured mDL data.

3.2.5 Non-verified subscriber information

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

3.2.6 Validation of authority

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 3.2.3.2.1 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.

3.2.7 Criteria for interoperation

The CA SHALL disclose all Cross 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 Certificate at issue).

3.2.8 Reliability of verification sources

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 request

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; and
2. An executed Subscriber Agreement and/or Terms of Use.

The Certificate Request and Subscriber Agreement or Terms of Use SHALL be in a form prescribed by the CA and SHALL comply with these Requirements including Section 9.6.3. The CA SHOULD obtain any additional documentation the CA determines necessary to fulfill these Requirements.

The Certificate Request SHALL 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.

One Certificate Request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the validation reuse periods described 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.

A CA may rely on a previously verified Certificate Request to issue a replacement Certificate if:

1. The previous Certificate being referenced was not revoked;
2. The expiration date of the replacement Certificate is the same as the previous Certificate being referenced; and
3. The Subject Information of the Certificate is the same as the previous Certificate being referenced.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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 3.2.2.1 or Section 3.2.2.3 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 3.2.2.1, 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 3.2.2.2 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 3.2.3 SHALL be obtained no more than 825 days prior to issuing the Certificate.

   Validation of authority in accordance with Section 3.2.6 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 3.2.4 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

4.2.2.1 Certification authority authorization

Starting on September 15, 2024 the CA SHALL state its policy or practice on processing CAA Records for Mailbox Addresses in Section 4.2 of its CP and/or CPS. That policy SHALL be consistent with these Requirements and SHALL clearly specify the set of Issuer Domain Names that the CA recognizes in CAA `issuemail` records as permitting it to issue.Starting on September 15, 2024 prior to issuing a Certificate that includes a Mailbox Address, the CA SHOULD retrieve and process CAA records in accordance with Section 4 of RFC 9495: Certification Authority Authorization (CAA) Processing for Email Addresses.

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

Some methods relied upon for validating the Applicant's control over the domain portion of the Mailbox Address to be used in the Certificate (see Section 3.2.2.1 and Section 3.2.2.3) require CAA records to be retrieved and processed from additional remote Network Perspectives before Certificate issuance (see Section 4.2.2.2). To corroborate the Primary Network Perspective, a remote Network Perspective's CAA check response MUST be interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. Additionally, a CA MAY consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in this section.

When processing CAA records, CAs SHALL process the `issuemail` property tag as specified in RFC 9495. Additional property tags MAY be supported, but SHALL NOT conflict with or supersede the authorizations to issue S/MIME Certificates as specified in the `issuemail` property tag.

If the CA issues a Certificate following a CAA check, they SHALL 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.

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

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

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

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

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

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

4.2.2.1.1 DNSSEC validation of CAA records

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

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

Effective March 15, 2026 CAs MUST NOT use local policy to disable DNSSEC validation on any DNS query associated with CAA record lookups.

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

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

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

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

4.2.2.2 Multi-perspective issuance corroboration

CAs SHOULD implement Section 3.2.2.9 of the TLS Baseline Requirements before March 15, 2025.

Effective May 15, 2025 CAs SHALL implement Section 3.2.2.9 of the TLS Baseline Requirements. This optional delay to the Phased Implementation Timeline for MPIC is intended to assist S/MIME Certificate Issuers with no TLS MPIC obligations.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

4.3.1.1 Manual authorization of certificate issuance for Root CAs

Certificate issuance by the Root CA SHALL require at least two individuals authorized by the CA (i.e., the CA system operator, system officer, or PKI administrator) one of whom deliberately issues a direct command in order for the Root CA to perform a Certificate signing operation.

4.3.1.2 Linting of to-be-signed Certificate content

It is considered best practice for the CA to implement a Linting process to test the technical conformity of each to-be-signed artifact prior to signing it.

Effective March 15, 2025 the CA SHOULD implement a Linting process testing compliance with these Requirements for S/MIME Certificates. Effective September 15, 2025 the CA SHALL implement a Linting process testing compliance with these Requirements for S/MIME Certificates.

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

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

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

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

- Creating new or improving existing lints;
- Reporting potentially inaccurate linting results as bugs;
- Notifying maintainers of Linting software of checks that are not covered by existing lints;
- Updating documentation of existing lints; and
- Generating test Certificates for positive/negative tests of specific lints.

4.3.1.3 Linting of issued certificates

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

4.3.2 Notification to subscriber by the CA of issuance of certificate

No stipulation.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

No stipulation.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

See Section 9.6.3, provisions 2. and 4.

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

No stipulation.

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 if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
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);
5. The CA obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon.

The CA SHOULD revoke a Certificate within 24 hours and SHALL revoke a Certificate within 5 days if one or more of the following occurs:

6. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
7. The CA obtains evidence that the Certificate was misused;
8. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
9. The CA is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);
10. The CA is made aware of a material change in the information contained in the Certificate;
11. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's CP and/or CPS;
12. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
13. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
14. Revocation is required by the CA's CP and/or CPS; or
15. 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.

4.9.1.2 Reasons for revoking a subordinate CA certificate

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that

Subordinate CA has not complied with this document or the applicable CP and/or 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 these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's CP and/or 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 a Certificate.

4.9.3 Procedure for revocation request

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

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

4.9.4 Revocation request grace period

No stipulation.

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 on which the CA will revoke the Certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation SHALL 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 should be addressed with higher priority); 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: the CA SHALL update and reissue CRLs at least once every seven days, and the value of the `nextUpdate` field SHALL 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 twelve months; and
2. within 24 hours after revoking a Subordinate CA Certificate.

The value of the `nextUpdate` field SHALL NOT be more than twelve months 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

When provided, OCSP responses SHALL conform to RFC 6960 and/or RFC 5019. OCSP responses SHALL 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 SHALL contain the ocspSigning EKU (1.3.6.1.5.5.7.3.9) and an extension of type `id-pkix-ocsp-nocheck`, as defined by RFC 6960.

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 SHALL have a validity interval greater than or equal to eight hours;
2. OCSP responses SHALL have a validity interval less than or equal to ten days;
3. For OCSP responses with validity intervals less than sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate; and

4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol 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 OCSP:

1. at least every twelve months; 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 7.1.5, the responder SHALL NOT respond with a "good"status for such requests.

A Certificate serial number within an OCSP request is "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 "unused"if otherwise.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

See Section 4.9.1.

4.9.13 Circumstances for suspension

See Section 7.2.2 for restrictions on use of suspension. The CA implementing suspension SHALL only use the `CRLreason` of certificateHold (6). The CA SHALL describe its suspension practices for Subscriber Certificates in the CA's CP and/or CPS.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

4.10.1 Operational characteristics

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

4.10.2 Service availability

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

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

The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

The CA MAY escrow the Subscriber's Private Key as specified in the CA's CP and/or 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 CP and/or CPS.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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 SHALL 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 SHALL include an annual Risk Assessment that:

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

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

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 the CA's CP and/or CPS), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.

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

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

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

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

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 these Requirements.

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. Certificate requests, renewal, and re-key requests, and revocation;
iii. Approval and rejection of Certificate Requests;
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. Certificate requests, renewal, and re-key requests, and revocation;
   ii. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
   iii. Approval and rejection of Certificate Requests;
   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. Relevant router and firewall activities (as described in Section 5.4.1.1); and
   vii. Entries to and exits from the CA facility.

Log records SHALL include at least the following elements:

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

5.4.1.1 Router and firewall activities logs

Logging of router and firewall activities necessary to meet the requirements of Section 5.4.1, Subsection 3.6 MUST at a minimum include:

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2 Frequency of processing audit log

No stipulation.

5.4.3 Retention period for audit log

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

1. CA Certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of:

    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 these Requirements set the minimum retention period, the CA MAY choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past audit log events.

5.4.4 Protection of audit log

No stipulation.

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 SHALL include an annual Risk Assessment that:

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

5.5 Records archival

5.5.1 Types of records archived

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

Additionally, the CA and each Delegated Third Party SHALL archive:

1. Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and
2. Documentation related to their verification, issuance, and revocation of Certificate Requests and Certificates.

5.5.2 Retention period for archive

Archived audit logs (as set forth in Section 5.5.1 SHALL be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

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

1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in Section 5.5.1); and
2. All archived documentation relating to the verification, issuance, and revocation of Certificate Requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of:
    1. such records and documentation were last relied upon in the verification, issuance, or revocation of Certificate Requests and Certificates; or
    2. the expiration of the Subscriber Certificates relying upon such records and documentation.

Note: While these Requirements set the minimum retention period, the CA MAY choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past records archived.

5.5.3 Protection of archive

No stipulation.

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

CA operators SHALL have an Incident Response Plan and a Disaster Recovery Plan.

The CA SHALL document a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The CA is not required to publicly

disclose its business continuity plans but SHALL make its business continuity plan and security plans available to the CA's auditors upon request. The CA SHALL annually test, review, and update these procedures.

The business continuity plan SHALL include:

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

5.7.2 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 CA 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. either (i) have a Qualified Auditor witness the CA Key Pair generation process, or (ii) video-record the entire CA Key Pair generation process for review by its Qualified Auditor.

In all cases, the CA SHALL:

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

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/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;

3. The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. The CA has previously been 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).

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.

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

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:

1. Transport the Private Key in hardware with an activation method that is equivalent to 128 bits of encryption, where 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; or
2. Encrypt the Private Key with at least 112 bits of encryption strength.

Illustrative examples include:

- Using a 128-bit AES key to wrap the Private Key.
- Storing the key in a PKCS 12 file encrypted using a password and algorithm whose combination provides at least 112 bits of encryption strength.
- Transporting the Private Key and/or PKCS 12 file and/or activation material via a TLS or other authenticated and encrypted network connection with at least 112 bits of encryption strength.
- Other approaches that meet the requirements are allowed.

The CA or Delegated Third Party SHALL NOT store Subscriber Private Keys in clear text.

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.

For EdDSA key pairs, the CA SHALL:

- Ensure that the key represents a valid point on the curve25519 or curve 448 elliptic curve.

For ML-DSA key pairs, the CA SHALL:

- Ensure the Key uses one of the following parameter sets:
  - ML-DSA-44 (OID: 2.16.840.1.101.3.4.3.17), or
  - ML-DSA-65 (OID: 2.16.840.1.101.3.4.3.18), or
  - ML-DSA-87 (OID: 2.16.840.1.101.3.4.3.19).

For ML-KEM key pairs, the CA SHALL:

- Ensure the Key uses one of the following parameter sets:
  - ML-KEM-512 (OID: 2.16.840.1.101.3.4.4.1), or
  - ML-KEM-768 (OID: 2.16.840.1.101.3.4.4.2), or
  - ML-KEM-1024 (OID: 2.16.840.1.101.3.4.4.3).

No other algorithms or key sizes are permitted.

6.1.6 Public key parameters generation and quality checking

For RSA key pairs: 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. (See NIST SP 800-89, Section 5.3.3.)

For ECDSA key pairs: 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. (See NIST SP 800-56A: Revision 2, Sections 5.6.2.3.2 and 5.6.2.3.3.)

For EdDSA key pairs: no stipulation.

For ML-DSA key pairs: no stipulation.

For ML-KEM key pairs: no stipulation.

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

Private Keys corresponding to Root CA Certificates SHALL 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 Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

6.2 Private key protection and cryptographic module engineering controls

The CA SHALL implement physical and logical safeguards to prevent unauthorized Certificate issuance. Protection of the CA Private Key outside the validated system or device specified above

SHALL consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. The CA SHALL encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic module standards and controls

No stipulation.

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

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

See Section 5.2.2.

6.2.5 Private key archival

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

6.2.6 Private key transfer into or from a cryptographic module

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

6.2.7 Private key storage on cryptographic module

The CA SHALL protect its Private Key in a system or device that has been validated as meeting at least FIPS 140-2 level 3, FIPS 140-3 level 3, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

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

No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

Generation	Certificate Maximum Validity Period
Strict and Multipurpose	825 days
Legacy	1185 days

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

Where escrow is supported in accordance with Section 4.12, the CA MAY retain Subscriber Private Keys past the Certificate Maximum Validity Period.

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

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

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, Section 6.1.5, and Section 6.1.6.

CAs SHALL generate non-sequential Certificate serial numbers greater than zero (0) and less than 2^159 containing at least 64 bits of output from a CSPRNG.

7.1.1 Version number(s)

Certificates SHALL be of type X.509 v3.

7.1.2 Certificate content and extensions; application of RFC 6818

This section specifies the additional requirements for Certificate content and extensions for Certificates.

7.1.2.1 Root CA certificates

a. `basicConstraints` (SHALL be present)

   This extension SHALL be marked critical. The `cA` field SHALL be set true. The `pathLenConstraint` field SHOULD NOT be present.

b. `keyUsage` (SHALL be present)

   This extension SHALL be marked critical. Bit positions for `keyCertSign` and `cRLSign` SHALL be set. If the Root CA Private Key is used for signing OCSP responses, then the `digitalSignature` bit SHALL be set.

c. `certificatePolicies` (SHOULD NOT be present)

   This extension SHOULD NOT be present.

d. `extKeyUsage` (SHALL NOT be present)

   This extension SHALL NOT be present.

e. `subjectKeyIdentifier` (SHALL be present)

   This extension SHALL NOT be marked critical. It SHALL contain a value that is included in the `keyIdentifier` field of the `authorityKeyIdentifier` extension in Certificates issued by the Root CA.

7.1.2.2 Subordinate CA certificates

The issuance of end entity S/MIME Certificates by Extant S/MIME CAs is described in Appendix B.

a. `certificatePolicies` (SHALL be present)

   This extension SHOULD NOT be marked critical.

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

If the value of this extension includes a `PolicyInformation` which contains a qualifier of type `id-qt-cps` (OID: 1.3.6.1.5.5.7.2.1), then the value of the qualifier SHALL be a HTTP or HTTPS URL for the Issuing CA's CP and/or CPS, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA. If a qualifier of type `id-qt-unotice` (OID: 1.3.6.1.5.5.7.2.2) is included, then it SHALL contain `explicitText` and SHALL NOT contain `noticeRef`.

b. `cRLDistributionPoints` (SHALL be present)

   This extension SHALL NOT be marked critical. It SHALL contain the HTTP URL of the CA's CRL service.

c. `authorityInformationAccess` (SHOULD be present)

   This extension SHALL NOT be marked critical.

   It SHOULD contain the HTTP URL of the Issuing CA Certificate (`accessMethod` = 1.3.6.1.5.5.7.48.2). It MAY contain the HTTP URL of the Issuing CA OCSP responder (`accessMethod` = 1.3.6.1.5.5.7.48.1).

d. `basicConstraints` (SHALL be present)

   This extension SHALL be marked critical. The `cA` field SHALL be set true. The `pathLenConstraint` field MAY be present.

e. `keyUsage` (SHALL be present)

   This extension SHALL be marked critical. Bit positions for `keyCertSign` and `cRLSign` SHALL be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the `digitalSignature` bit SHALL be set.

f. `nameConstraints` (MAY be present)

   This extension SHOULD be marked critical[1].

g. `extKeyUsage` (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[2].

   For Subordinate CA Certificates that will be used to issue S/MIME Certificates, the value `id-kp-emailProtection` SHALL be present. The values `id-kp-serverAuth`, `id-kp-codeSigning`, `id-kp-timeStamping`, and `anyExtendedKeyUsage` SHALL NOT be present. Other values MAY be present.

[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.

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

h. `authorityKeyIdentifier` (SHALL be present)

This extension SHALL NOT be marked critical. It SHALL contain a `keyIdentifier` field and it SHALL NOT contain a `authorityCertIssuer` or `authorityCertSerialNumber` field.

i. `subjectKeyIdentifier` (SHALL be present)

This extension SHALL NOT be marked critical. It SHALL contain a value that is included in the `keyIdentifier` field of the `authorityKeyIdentifier` extension in Certificates issued by the Subordinate CA.

7.1.2.3 Subscriber certificates

a. `certificatePolicies` (SHALL be present)

This extension SHOULD NOT be marked critical. It SHALL include exactly one of the reserved `policyIdentifiers` listed in Section 7.1.6.1, and MAY contain one or more identifiers documented by the CA in its CP and/or CPS.

If the value of this extension includes a `PolicyInformation` which contains a qualifier of type `id-qt-cps` (OID: 1.3.6.1.5.5.7.2.1), then the value of the qualifier SHALL be a HTTP or HTTPS URL for the Issuing CA's CP and/or CPS, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA. If a qualifier of type `id-qt-unotice` (OID: 1.3.6.1.5.5.7.2.2) is included, then it SHALL contain `explicitText` and SHALL NOT contain `noticeRef`.

b. `cRLDistributionPoints` (SHALL be present)

This extension SHOULD NOT be marked critical. It SHALL contain at least one `distributionPoint` whose `fullName` value includes a GeneralName of type `uniformResourceIdentifier` that includes a URI where the Issuing CA's CRL can be retrieved.

Generation	Allowed URI scheme
Strict and Multipurpose	Every `uniformResourceIdentifier` SHALL have the URI scheme HTTP. Other schemes SHALL NOT be present.
Legacy	At least one `uniformResourceIdentifier` SHALL have the URI scheme HTTP. Other schemes (LDAP, FTP, ⋯) MAY be present.

c. `authorityInformationAccess` (SHOULD be present)

This extension SHALL NOT be marked critical.

1. `id-ad-ocsp`

The `authorityInformationAccess` extension MAY contain one or more `accessMethod` values of type `id-ad-ocsp` that specifies the URI of the Issuing CA's OCSP responder.

Generation	Allowed URI scheme
Strict and Multipurpose	When provided, every `accessMethod` SHALL have the URI scheme HTTP. Other schemes SHALL NOT be present.
Legacy	When provided, at least one `accessMethod` SHALL have the URI scheme HTTP. Other schemes (LDAP, FTP, ⋯) MAY be present.

2. `id-ad-caIssuers`

   The `authorityInformationAccess` extension SHOULD contain at least one `accessMethod` value of type `id-ad-caIssuers` that specifies the URI of the Issuing CA's Certificate.

Generation	Allowed URI scheme
Strict and Multipurpose	When provided, every `accessMethod` SHALL have the URI scheme HTTP. Other schemes SHALL NOT be present.
Legacy	When provided, at least one `accessMethod` SHALL have the URI scheme HTTP. Other schemes (LDAP, FTP, ⋯) MAY be present.

d. `basicConstraints` (optional)

   This extension MAY be present. The `cA` field SHALL NOT be true. `pathLenConstraint` field SHALL NOT be present.

e. `keyUsage` (SHALL be present)

   This extension SHOULD be marked critical.

Generation	`rsaEncryption`	`id-ecPublicKey`	`id-Ed25519` and `id-Ed448`
Strict	For signing only, bit positions SHALL be set for `digitalSignature` and MAY be set for `nonRepudiation`.For key management only, bit positions SHALL be set for `keyEncipherment`.For dual use, bit positions SHALL be set for `digitalSignature` and `keyEncipherment` and MAY be set for `nonRepudiation`.	For signing only, bit positions SHALL be set for `digitalSignature` and MAY be set for `nonRepudiation`.For key management only, bit positions SHALL be set for `keyAgreement` and MAY be set for `encipherOnly` or `decipherOnly`.For dual use, bit positions SHALL be set for `digitalSignature` and `keyAgreement`, MAY be set for `nonRepudiation`, and MAY be set for `encipherOnly` or `decipherOnly` (only if `keyAgreement` is set).	Bit positions SHALL be set for `digitalSignature` and MAY be set for `nonRepudiation`.
Multipurpose and Legacy	For signing only, bit positions SHALL be set for `digitalSignature` and MAY be set for `nonRepudiation`.For key management only, bit positions SHALL be set for `keyEncipherment` and MAY be set for `dataEncipherment`.For dual use, bit positions SHALL be set for `digitalSignature` and `keyEncipherment`, MAY be set for `nonRepudiation`, and MAY be set for `dataEncipherment`.	For signing only, bit positions SHALL be set for `digitalSignature` and MAY be set for `nonRepudiation`.For key management only, bit positions SHALL be set for `keyAgreement` and MAY be set for `encipherOnly` or `decipherOnly`.For dual use, bit positions SHALL be set for `digitalSignature` and `keyAgreement`, MAY be set for `nonRepudiation`, and MAY be set for `encipherOnly` or `decipherOnly` (only if `keyAgreement` is set).	Bit positions SHALL be set for `digitalSignature` and MAY be set for `nonRepudiation`.

Other bit positions SHALL NOT be set.

Generation	id-ml-dsa	id-ml-kem
Legacy and Multipurpose and Strict	Bit positions SHALL be set for digitalSignature and MAY be set for nonRepudiation. Other bit positions SHALL NOT be set.	keyEncipherment SHALL be the only key usage set.

f. extKeyUsage (SHALL be present)

Generation	KeyPurposeId
Strict Multipurpose and Legacy	id-kp-emailProtection SHALL be present. Other values SHALL NOT be present. id-kp-emailProtection SHALL be present. Other values MAY be present.

The values id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, and anyExtendedKeyUsage SHALL NOT be present.

g. authorityKeyIdentifier (SHALL be present)

This extension SHALL NOT be marked critical. The keyIdentifier field SHALL be present. authorityCertIssuer and authorityCertSerialNumber fields SHALL NOT be present.

h. subjectAlternativeName (SHALL be present)

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.

i. smimeCapabilities (optional)

This extension MAY be present and SHALL NOT be marked critical. May indicate cryptographic capabilities of the sender of a signed S/MIME message, defined in RFC 4262.

j. subjectDirectoryAttributes (optional)

Generation	subjectDirectoryAttributes
Strict and Multipurpose Legacy	Prohibited MAY be present and SHALL NOT be marked critical.

This extension MAY be present. 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.

k. qcStatements (optional)

This extension MAY be present and SHALL NOT be marked critical. 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.

l. Legal Entity Identifier (optional)

Generation	LEI
`Mailbox-validated`	Prohibited
`Organization-validated`	LEI (1.3.6.1.4.1.52266.1) MAY be present and SHALL NOT be marked critical. Role (1.3.6.1.4.1.52266.2) SHALL NOT be present.
`Sponsor-validated`	LEI (1.3.6.1.4.1.52266.1) or for role (1.3.6.1.4.1.52266.2) MAY be present and SHALL NOT be marked critical.
`Individual-validated`	Prohibited

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.

In cases where the "role"LEI is used, the CA SHALL verify that the LEI data reference is assigned to the Individual Subject whose identity has been verified in accordance with Section 3.2.4.

m. Adobe Extensions (optional)

Generation	Adobe Extensions
Strict	Prohibited
Multipurpose and Legacy	MAY be present and SHALL NOT be marked critical. May include the Adobe Time-stamp X509 extension (1.2.840.113583.1.1.9.1) or the Adobe ArchiveRevInfo extension (1.2.840.113583.1.1.9.2)

n. `subjectKeyIdentifier` (SHOULD be present)

This extension SHALL NOT be marked critical. It SHOULD contain a value that is derived from the Public Key included in the Subscriber Certificate.

7.1.2.4 All 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 7.1.2.1, Section 7.1.2.2, or Section 7.1.2.3 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 these Requirements, 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 CP and/or 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
iii. the extension is defined within an open standards specification and intended for use by other organizations. A Certificate that includes such an extension MUST conform to the specifications of the open standard and of these Requirements.

2. Field or extension values which have not been validated according to the processes and procedures described in these Requirements or the CA's CP and/or CPS.

7.1.3 Algorithm object identifiers

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to the `subjectPublicKeyInfo` field within a Certificate. 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 SHALL be present, and SHALL 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 SHALL be byte-for-byte identical with the following hex-encoded bytes: `300d06092a864886f70d0101010500`

Effective September 15, 2026 the CA SHALL NOT sign a certificate using a signature algorithm that incorporates SHA-1.

Prior to September 15, 2026 the CA SHALL revoke any unexpired Subordinate CA Certificate whose signature algorithm incorporates SHA-1.

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 SHALL use the `namedCurve` encoding.

- For P-256 keys, the `namedCurve` SHALL be secp256r1 (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, the `namedCurve` SHALL be secp384r1 (OID: 1.3.132.0.34).
- For P-521 keys, the `namedCurve` SHALL be secp521r1 (OID: 1.3.132.0.35).

When encoded, the `AlgorithmIdentifier` for ECDSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For P-256 keys, `301306072a8648ce3d020106082a8648ce3d030107`.
- For P-384 keys, `301006072a8648ce3d020106052b81040022`.
- For P-521 keys, `301006072a8648ce3d020106052b81040023`.

7.1.3.1.3 EdDSA

The CA SHALL indicate an EdDSA key using one of the following algorithm identifiers below:

- For curve25519 keys, the `algorithm` SHALL be id-Ed25519 (OID: 1.3.101.112).
- For curve448 keys, the `algorithm` SHALL be id-Ed448 (OID: 1.3.101.113).

The parameters for EdDSA keys SHALL be absent.

When encoded, the `AlgorithmIdentifier` for EdDSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For Curve25519 keys, `300506032b6570`.
- For Curve448 keys, `300506032b6571`.

7.1.3.2.4 ML-DSA

The CA SHALL indicate an ML-DSA key using one of the following algorithm identifiers below:

- ML-DSA-44 (OID: 2.16.840.1.101.3.4.3.17), or
- ML-DSA-65 (OID: 2.16.840.1.101.3.4.3.18), or
- ML-DSA-87 (OID: 2.16.840.1.101.3.4.3.19).

The parameters for ML-DSA keys SHALL be absent. The CA MUST NOT use HashML-DSA; only "pure"ML-DSA is permitted.

When encoded, the `AlgorithmIdentifier` for ML-DSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For ML-DSA-44, `300b060960864801650304031`1.
- For ML-DSA-65, `300b060960864801650304031`2.
- For ML-DSA-87, `300b060960864801650304031`3.

7.1.3.2.5 ML-KEM

The CA SHALL indicate an ML-KEM key using one of the following algorithm identifiers below:

- ML-KEM-512 (OID: 2.16.840.1.101.3.4.4.1), or
- ML-KEM-768 (OID: 2.16.840.1.101.3.4.4.2), or
- ML-KEM-1024 (OID: 2.16.840.1.101.3.4.4.3).

The parameters for ML-KEM keys SHALL be absent.

When encoded, the `AlgorithmIdentifier` for ML-KEM keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For ML-KEM-512, `300b060960864801650304040`1.
- For ML-KEM-768, `300b060960864801650304040`2.
- For ML-KEM-1024, `300b060960864801650304040`3.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a CA Private Key SHALL 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.
- The `signature` field of a TBSCertificate (for example, as used by a Certificate).
- The `signatureAlgorithm` field of a CertificateList
- The `signature` field of a TBSCertList
- The `signatureAlgorithm` field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

The CA SHALL use one of the following signature algorithms and encodings. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the specified hex-encoded bytes.

- RSASSA-PKCS1-v1_5 with SHA-256:

  Encoding: `300d06092a864886f70d01010b0500`.

- RSASSA-PKCS1-v1_5 with SHA-384:

  Encoding: `300d06092a864886f70d01010c0500`.

- RSASSA-PKCS1-v1_5 with SHA-512:

  Encoding: `300d06092a864886f70d01010d0500`.

- RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes:

  Encoding:

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

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

  Encoding:

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

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

  Encoding:

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

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 SHALL use ECDSA with SHA-256. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040302`.

If the signing key is P-384, the signature SHALL use ECDSA with SHA-384. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040303`.

If the signing key is P-521, the signature SHALL use ECDSA with SHA-512. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040304`.

7.1.3.2.3 EdDSA

The CA SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is Curve25519, the signature algorithm SHALL be id-Ed25519 (OID: 1.3.101.112). When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300506032b6570`.

If the signing key is Curve448, the signature algorithm SHALL be id-Ed448 (OID: 1.3.101.113). When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300506032b6571`.

7.1.3.2.4 ML-DSA

The CA SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is ML-DSA-44, the signature algorithm SHALL be id-ml-dsa-44 (OID: 2.16.840.1.101.3.4.3.17). When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300b0609608648016503040311`.

If the signing key is ML-DSA-65, the signature algorithm SHALL be id-ml-dsa-65 (OID: 2.16.840.1.101.3.4.3.18). When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300b0609608648016503040312`.

If the signing key is ML-DSA-87, the signature algorithm SHALL be id-ml-dsa-87 (OID: 2.16.840.1.101.3.4.3.19). When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300b0609608648016503040313`.

7.1.4 Name forms

Attribute values SHALL be encoded according to RFC 5280.

7.1.4.1 Name encoding

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA Certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate SHALL be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

7.1.4.2 Subject information - subscriber certificates

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

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 Subject alternative name extension

Certificate Field: `extensions:subjectAltName`
Required/Optional: SHALL be present
Contents: 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 9598

All Mailbox Addresses in the `subject` field or entries of type `directoryName` 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 `directoryName` provided that the information contained in the `Name` complies with the requirements set forth in Sections 7.1.4.2.2 through 7.1.4.2.6, according to the Certificate Type. Additionally, information contained in the `Name` SHALL be validated according to Section 3.1, Section 3.2.3, and/or Section 3.2.4, as appropriate for the Certificate Type.

For Legacy and Multipurpose 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 Subject distinguished name fields

a. **Certificate Field:** `subject:commonName` (OID 2.5.4.3)
Contents: If present, this attribute SHALL contain one of the following values verified in accordance with Section 3.2.

Certificate Type	Contents
`Mailbox-validated`	Mailbox Address
`Organization-validated`	`subject:organizationName` or Mailbox Address
`Sponsor-validated`	Personal Name, Pseudonym, or Mailbox Address
`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 `subject:givenName` and/or `subject: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 3.2.4.

If present, the Mailbox Address SHALL contain a `rfc822Name` or `otherName` value of type `id-on-SmtpUTF8Mailbox` from `extensions:subjectAltName`.

If the `subject:commonName` contains a Pseudonym, then the `subject:givenName` and/or `subject:surname` attributes SHALL NOT be present. If present, the Pseudonym SHALL contain the `subject:pseudonym` if that Subject attribute is also present.

If the `subject:commonName` contains a Personal Name, then the `subject:pseudonym` attribute SHALL NOT be present.

Note: Like all other Certificate attributes, `subject:commonName` and `subject:emailAddress` SHALL comply with the attribute upper bounds defined in RFC 5280.

Additional specifications for naming are provided in Section 3.1.

b. **Certificate Field:** `subject:organizationName` (OID 2.5.4.10)
Contents: If present, the `subject:organizationName` field SHALL contain the Subject's full legal organization name and/or an Assumed Name as verified under Section 3.2.3. If both are included, the Assumed Name SHALL appear first, followed by the full legal organization name in parentheses. 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".

c. **Certificate Field:** `subject:organizationalUnitName` (OID: 2.5.4.11)
Contents: If present, the CA SHALL confirm that the `subject:organizationalUnitName` is the full legal organization name of an Affiliate of the `subject:organizationName` in the Certificate and has been verified in accordance with the requirements of Section 3.2.3. 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.

d. **Certificate Field:** `subject:organizationIdentifier` (2.5.4.97)
Contents: If present, the `subject:organizationIdentifier` field SHALL contain a Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme. The Registration Reference SHOULD be unique where the Registration Scheme and jurisdiction provide unique identifiers.

   The `subject: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 3.2.3.

   If the Registration Reference is assigned at the country level, the Registration Scheme SHALL be identified using the following structure in the presented order:

   - 3 character Registration Scheme identifier; and
   - 2 character ISO 3166-1 country code for the nation in which the Registration Scheme is operated, or as described in Note 1; and
   - a hyphen-minus "-"(0x2D (ASCII), U+002D (UTF-8)); and
   - Registration Reference allocated in accordance with the identified Registration Scheme (or as described in Note 3).

If the Registration Reference is assigned at the subdivision (state or province) level and is not unique at the national level, the Registration Scheme SHALL be identified using the following structure in the presented order:

```
* 3 character Registration Scheme identifier; and
* 2 character ISO 3166-1 country code for the nation in which the Registration Sche
* plus "+" (0x2B (ASCII), U+002B (UTF-8)); and
* up-to-3 character ISO 3166-2 identifier for the subdivision; and
```

```
* a hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
* Registration Reference allocated in accordance with the identified Registration
```

Registration References MAY contain hyphens but Registration Schemes, ISO 3166-1 country codes, and ISO 3166-2 identifiers SHALL NOT contain hyphens. 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, Registration Reference at Country
* `NTRUS+CA-12345678` (NTR Scheme, United States - California, Registration Refer
* `PSDBE-NBB-1234.567.890` (PSD Scheme, Belgium, National Competent Authority ide
* `VATEL-123456789` (VAT Scheme, Greece using EU Council Directive 2006/112/EC as
```

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

1. 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
2. Further verify the Registration Reference matches other information verified in accordance with Section 3.2.3.

Note 1: With the exception of the LEI and INT Registration Schemes, if a `subject:countryName` is present in the Certificate the country code used in the Registration Scheme identifier SHALL match that of the `subject:countryName` in the Certificate.

For the VAT Registration Scheme, the country prefix described in Article 215 of EU Council Directive 2006/112/EC, as amended, MAY be used instead of the ISO 3166-1 country code. If the country prefix described in Article 215 of EU Council Directive 2006/112/EC is used, the `subject:countryName` attribute, if present, SHALL contain the corresponding ISO 3166-1 country code.

For the LEI Registration Scheme, the ISO 3166-1 code "XG"SHALL be used.

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

```
* For Government Entities, the CA SHALL enter the Registration Scheme identifier '
1 country code for the nation in which the Government Entity is located.  If the Gov
8)) followed by an ISO 3166-2 identifier for the subdivision (up to three alphanume
* For International Organization Entities, the CA SHALL enter the Registration Sch
1 code "XG". An International Organization Entity is founded by a constituent docu

For example:
* GOVUS (Government Entity, United States)
* GOVUS+CA (Government Entity, United States - California)
* INTXG (International Organization)
```

Note 3: For the NTR Registration Scheme, when the Organization or Legal Entity is registered in the European Union or the European Economic Area, the Registration Reference MAY use the EUID identifier. When the Organization or Legal Entity is registered in Germany, the Registration Reference SHOULD use the EUID identifier. The structure of the EUID SHALL be as follows:

```
* 2 character ISO 3166-1 country code, which must match the country code used in th
* the business register identifier for the particular section or office of the dome
```

```
* dot-sign '.' (U+002E); and
* the Registration Reference allocated by the domestic register.

For example:
* NTRDE-DER3306.HRB12345 (DE is the country code for Germany, R3306 is the busines
assigned Registration Reference).
```

e. **Certificate Field:** `subject:givenName` (2.5.4.42) and/or `subject:surname` (2.5.4.4)
Contents: If present, the `subject:givenName` field and `subject:surname` field SHALL contain a Natural Person Subject's name as verified under Section 3.2.4. 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.

f. **Certificate Field:** `subject:pseudonym` (2.5.4.65)
Contents: The `subject:pseudonym` 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.

g. **Certificate Field:** `subject:serialNumber` (2.5.4.5)
Contents: If present, the `subject:serialNumber` MAY be used to contain an identifier assigned by the CA or RA to identify and/or to disambiguate the Subscriber.

   In addition, the `subject:serialNumber` 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 A 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 3.2.4.

h. **Certificate Field:** `subject:emailAddress` (1.2.840.113549.1.9.1) **Contents:** If present, the `subject:emailAddress` SHALL contain a single Mailbox Address as verified under Section 3.2.2.

i. **Certificate Field:** `subject:title` (2.5.4.12) **Contents:** If present, the `subject:title` field SHALL contain only a organizational role/title or a regulated professional designation verified according to Section 3.2.4.

j. **Certificate Field:** Number and street: `subject:streetAddress` (OID: 2.5.4.9)
Contents: If present, the `subject:streetAddress` field SHALL contain the Subject's street address information as verified under Section 3.2.3 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.4 for Individual-validated Certificate Types. The `subject:streetAddress` field SHALL only be used if the `subject:localityName` or `subject:stateOrProvinceName` field is present.

k. **Certificate Field:** `subject:localityName` (OID: 2.5.4.7)
Contents: If present, the `subject:localityName` field SHALL contain the Subject's locality information as verified under Section 3.2.3 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.4 for Individual-validated Certificate Types. If the `subject:countryName` field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2 (n), the `subject:localityName` field MAY contain the Subject's locality and/or state or province information. The `subject:localityName` field

SHALL only be used if the `subject:countryName` field is present.

l. **Certificate Field:** `subject:stateOrProvinceName` (OID: 2.5.4.8)
Contents: If present, the `subject:stateOrProvinceName` field SHALL contain the Subject's state or province information as verified under Section 3.2.3 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.4 for Individual-validated Certificate Types. If the `subject:countryName` field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2 (n), the `subject:stateOrProvinceName` field MAY contain the full name of the Subject's country information. The `subject:stateOrProvinceName` field SHALL only be used if the `subject:countryName` field is present.

m. **Certificate Field:** `subject:postalCode` (OID: 2.5.4.17)
Contents: If present, the `subject:postalCode` field SHALL contain the Subject's zip or postal information as verified under Section 3.2.3 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.4 for Individual-validated Certificate Types. The `subject:postalCode` field SHALL only be used if the `subject:countryName` field is present.

n. **Certificate Field:** `subject:countryName` (OID: 2.5.4.6)
Contents: If present, the `subject:countryName` SHALL contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.3 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.4 for Individual-validated Certificate Types. 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.

7.1.4.2.3 Subject DN attributes for mailbox-validated profile

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

7.1.4.2.4 Subject DN attributes for organization-validated profile

Attribute	Legacy	Multipurpose	Strict
`commonName`	MAY	MAY	MAY
`organizationName`	SHALL	SHALL	SHALL

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

7.1.4.2.5 Subject DN attributes for sponsor-validated profile

Attribute	Legacy (See Note 1)	Multipurpose (See Note 2)	Strict (See Note 2)
commonName	MAY	MAY	MAY
organizationName	SHALL	SHALL	SHALL
organizationalUnitName	MAY	MAY	MAY
organizationIdentifier	SHALL	SHALL	SHALL
givenName	MAY	MAY	MAY
surname	MAY	MAY	MAY
pseudonym	MAY	MAY	MAY
serialNumber	MAY	MAY	MAY
emailAddress	MAY	MAY	MAY
title	MAY	MAY	MAY
streetAddress	MAY	MAY	SHALL NOT
localityName	MAY	MAY	MAY
stateOrProvinceName	MAY	MAY	MAY
postalCode	MAY	MAY	SHALL NOT
countryName	MAY	MAY	MAY
Other	MAY	SHALL NOT	SHALL NOT

Note:

1. Legacy Generation profiles MAY omit the `subject:givenName`, `subject:surname`, and `subject:pseudonym` attributes and include only the `subject:commonName` as described in Section 7.1.4.2.2(a).
2. Multipurpose and Strict Generation profiles SHALL include either `subject:givenName` and/or `subject:surname`, or the `subject:pseudonym`.

7.1.4.2.6 Subject DN attributes for individual-validated profile

Attribute	Legacy (See Note 1)	Multipurpose (See Note 2)	Strict (See Note 2)
commonName	MAY	MAY	MAY
organizationName	SHALL NOT	SHALL NOT	SHALL NOT
organizationalUnitName	SHALL NOT	SHALL NOT	SHALL NOT
organizationIdentifier	SHALL NOT	SHALL NOT	SHALL NOT
givenName	MAY	MAY	MAY
surname	MAY	MAY	MAY

Attribute	Legacy (See Note 1)	Multipurpose (See Note 2)	Strict (See Note 2)
`pseudonym`	MAY	MAY	MAY
`serialNumber`	MAY	MAY	MAY
`emailAddress`	MAY	MAY	MAY
`title`	MAY	MAY	MAY
`streetAddress`	MAY	MAY	SHALL NOT
`localityName`	MAY	MAY	MAY
`stateOrProvinceName`	MAY	MAY	MAY
`postalCode`	MAY	MAY	SHALL NOT
`countryName`	MAY	MAY	MAY
Other	MAY	SHALL NOT	SHALL NOT

Note:

1. Legacy Generation profiles MAY omit the `subject:givenName`, `subject:surname`, and `subject:pseudonym` attributes and include only the `subject:commonName` as described in Section 7.1.4.2.2(a).
2. Strict and Multipurpose Generation profiles SHALL include either `subject:givenName` and/or `subject:surname`, or the `subject:pseudonym`.

7.1.4.3 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 CP and/or CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.1 Subject distinguished name fields

a. **Certificate Field:** `subject:commonName` (OID 2.5.4.3)
Required/Optional: SHALL be present
Contents: 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.

b. **Certificate Field:** `subject:organizationName` (OID 2.5.4.10)
Required/Optional: SHALL be present
Contents: This field SHALL contain either the Subject CA's name or DBA as verified under Section 3.2.3.2.2. 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".

c. **Certificate Field:** `subject:countryName` (OID: 2.5.4.6)
Required/Optional: SHALL be present
Contents: 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.

d. Other Subject Attributes
Other attributes MAY be present within the subject field. If present, other attributes SHALL contain information that has been verified by the CA.

7.1.5 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 either a 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 3.2.2.3.
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 7.1.2.4.

7.1.6 Certificate policy object identifier

This section describes the content requirements for the Root CA, Subordinate CA, and Subscriber Certificates as they relate to the identification of Certificate Policy.

7.1.6.1 Reserved certificate policy identifiers

The following CA/Browser Forum Certificate Policy identifiers are reserved for use by CAs to assert that a Certificate complies with these Requirements.

Certificate Type	Generation	Policy Identifier
`Mailbox-validated`	Legacy	`2.23.140.1.5.1.1`
`Mailbox-validated`	Multipurpose	`2.23.140.1.5.1.2`
`Mailbox-validated`	Strict	`2.23.140.1.5.1.3`
`Organization-validated`	Legacy	`2.23.140.1.5.2.1`
`Organization-validated`	Multipurpose	`2.23.140.1.5.2.2`
`Organization-validated`	Strict	`2.23.140.1.5.2.3`
`Sponsor-validated`	Legacy	`2.23.140.1.5.3.1`
`Sponsor-validated`	Multipurpose	`2.23.140.1.5.3.2`
`Sponsor-validated`	Strict	`2.23.140.1.5.3.3`
`Individual-validated`	Legacy	`2.23.140.1.5.4.1`
`Individual-validated`	Multipurpose	`2.23.140.1.5.4.2`
`Individual-validated`	Strict	`2.23.140.1.5.4.3`

Effective July 15, 2025 S/MIME Subscriber Certificates SHALL NOT be issued using the Legacy Generation profiles 2.23.140.1.5.1.1, 2.23.140.1.5.2.1, 2.23.140.1.5.3.1, or 2.23.140.1.5.4.1.

7.1.6.2 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 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 these Requirements and MAY contain one or more identifiers documented by the Subordinate CA in its CP and/or CPS; and
2. SHALL NOT contain the `anyPolicy` identifier (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 `anyPolicy` identifier (2.5.29.32.0).

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

7.1.6.4 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) documented by the Issuing CA in its CP and/or CPS.

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(s)

No stipulation.

7.2.2 CRL and CRL entry extensions

If present, the `reasonCode` (OID 2.5.29.21) extension SHALL NOT be marked critical.

If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates, this CRL entry extension SHALL be present. The `CRLreason` of certificateHold (6) SHALL NOT be used for Root CA or Subordinate CA Certificates.

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 SHALL NOT be unspecified (0). If the reason for revocation is unspecified, CAs SHALL omit the reasonCode entry extension.

The Repository MAY include CRL entries that have a CRLreason of certificateHold (6) for Certificates that include the Certificate Policy identifiers for the Legacy or 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 SHALL indicate the most appropriate reason for revocation of the Certificate, as defined by the CA within its CP/CPS.

7.3 OCSP profile

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that Certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus SHALL be present.

The CRLReason indicated SHALL contain a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

The singleExtensions of an OCSP response SHALL 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 these Requirements;
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 CA/Browser Forum continues to improve the S/MIME Baseline Requirements while CPA Canada/WebTrust and ETSI also continue to update their audit criteria. We encourage all CAs to conform to each revision herein on the date specified without awaiting a corresponding update to an applicable audit criterion. In the event of a conflict between an existing audit criterion and a revision to the S/MIME Baseline Requirements, we will communicate with the audit community and attempt to resolve any uncertainty, and we will respond to implementation questions directed to questions@cabforum.org.

8.1 Frequency or circumstances of assessment

Certificates that are capable of being used to issue new Certificates SHALL either be Technically Constrained in line with Section 7.1.5 and audited in line with Section 8.8 only, or unconstrained and fully audited in line with all remaining requirements from this section. A Certificate is deemed as capable of being used to issue new Certificates if it contains an X.509v3 `basicConstraints` extension, with the `cA` boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period SHALL 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 S/MIME 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 S/MIME Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted S/MIME 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 319 403-1;
5. (For audits conducted in accordance with the WebTrust standard) licensed for WebTrust by CPA Canada;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

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. For Audit Periods starting before the Effective Date defined in Section 1.2.1 of the first version of these Requirements, "WebTrust for CAs v2.2.2 or newer"; or
2. For Audit Periods starting after the Effective Date defined in Section 1.2.1 of the first version of these Requirements, "WebTrust for CAs v2.2.2 or newer"AND "WebTrust for S/MIME Baseline Requirements v1.0.0 or newer"; or
3. For Audit Periods starting after April 1, 2025, "WebTrust for CAs v2.2.2 or newer"AND "WebTrust for S/MIME Baseline Requirements v1.0.0 or newer"AND "WebTrust for Network Security v2.0 or newer"; or
4. ETSI TS 119 411-6 v1.1.1 or newer, which includes normative references to ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 (the latest version of the referenced ETSI documents should be applied); or
5. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either
    a. encompasses all requirements of one of the above schemes; or
    b. consists of comparable criteria that are available for public review. Whichever scheme is chosen, it SHALL 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 SHALL be conducted by a Qualified Auditor, as specified in Section 8.2.

For Delegated Third Parties that are not Enterprise RAs, then the CA SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found above in this Section 8.4, that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's CP and/or CPS as described in Section 1.3.2. 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

No stipulation.

8.6 Communication of results

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

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

The Audit Report SHALL 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 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., ETSI EN 319 401, ETSI TS 119 411-6, ETSI EN 319 411-1 policy LCP, NCP or NCP+, ETSI EN 319 411-2 policy QCP-n, QCP-n-qscd, QCP-l or QCP-l-qscd; and
11. (For audits conducted in accordance with any of the ETSI standards) a statement to indicate that the auditor referenced the applicable CA/Browser Forum criteria, such as this document, and the version used.

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

The Audit Report SHALL be available as a PDF, and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report SHALL be uppercase letters and SHALL NOT contain colons, spaces, or line feeds. See https://www.ccadb.org/policy#51-audit-statement-content for more information.

8.7 Self audits

During the period in which the CA issues Certificates, the CA SHALL monitor adherence to its CP and/or CPS and these Requirements and control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample including a minimum of the greater of thirty (30) Certificates or three percent (3%) of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Effective March 15, 2025 the CA SHOULD use a Linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous linting performed on the same Certificates.

8.8 Review of delegated parties

Except for Delegated Third Parties, Enterprise RAs, and Technically Constrained Subordinate CAs that undergo an annual audit that meets the criteria specified in Section 8.4, the CA SHALL ensure the practices and procedures of delegated parties are in compliance with these Requirements and the relevant CP and/or CPS. The CA shall document the obligations of delegated parties and perform monitoring on at least an annual basis of the delegated parties' adherence with those obligations.

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

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 CP and/or CPS.

9.4.2 Information treated as private

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

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

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 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 CA Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate.

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

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

1. **Right to Use Mailbox 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 Mailbox Addresses listed in the Certificate's `subject` field and `subjectAltName` extension (or 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 CP and/or 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 CP and/or 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 (with the exception of the subject:serialNumber attribute);
   ii. followed the procedure when issuing the Certificate; and
   iii. accurately described the procedure in the CA's CP and/or 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 CP and/or 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 these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
6. **Status**: That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (Valid or Revoked) of all unexpired Certificates; and
7. **Revocation**: That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

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

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

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

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

1. Agreement to the Subscriber Agreement with the CA; or

2. 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 SHALL 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 SHALL 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 such as a 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 use the Certificate only on MailBox Addresses 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 CA's CP and/or CPS, or by these Requirements.

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 these Requirements, as if the tasks had not been delegated.

If the CA has issued and managed the Certificate in compliance with these Requirements and its CP and/or 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 the CA's CP and/or CPS. If the CA has not issued or managed the Certificate in compliance with these Requirements and its CP and/or 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 these Requirements or its CP and/or CPS, then the CA SHALL include the limitations on liability in the CA's CP and/or 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 agreed to distribute the Root CA Certificate do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, the CA SHALL defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

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.

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 these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which a CA operates or issues Certificates, a CA MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or Certificate issuances that are subject to that Law. In such event, the CA SHALL immediately (and prior to issuing a Certificate under the modified requirement) include in Section 9.16.3 of the CA's CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by the CA.

The CA SHALL 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 public@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

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

A.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, in addition to the GOV and INT identifiers described therein.

- **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 3166-1 country code SHALL be set to 'XG'.

A.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.
- **TAX**: For an identifier based on a personal tax reference number issued by a national tax authority.
- **TIN**: For an identifier based on Tax Identification Number issued to the Subject Individual according to the European Commission - Tax and Customs Union.
- **EID**: For an identifier based on electronic identification means (e.g., national eID or EU wallet)

Appendix B - 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, with the exception of the required revocation of any Certificate whose signature algorithm incorporates SHA-1 as described in Section 7.1.3.1.1.