Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

Version 3.8.0

XX YY, 2024

Table of Contents

1. INTRODUCTION

1.1 Overview

The Baseline Requirements for the Issuance and Management of Publicly-Trusted CodeSigning Certificates describe a subset of the requirements that a Certification Authority must meet to issue Code Signing Certificates.

The scope of these Requirements includes all “Code Signing Certificates”, as defined below, and associated Timestamp Authorities, and all Certification Authorities technically capable of issuing Code Signing Certificates, including any Root CA that is publicly trusted for code signing and all other CAs that might serve to complete the validation path to such Root CA. These Requirements do not address the issuance, use, maintenance, or revocation of Certificates by enterprises that operate their own Public Key Infrastructure for internal purposes only, where the Root CA Certificate is not distributed by any Application Software Supplier (as defined in the Baseline Requirements).

The primary goal of these Requirements is to enable trusted signing of code intended for public distribution, while addressing user concerns about the trustworthiness of signed objects and accurately identifying the software publisher. The Requirements also serve to inform users about the purpose of signed code, help users make informed decisions when relying on Certificates, help establish the legitimacy of signed code, help maintain the trustworthiness of software Platforms, help users make informed software choices, and limit the spread of malware. Code Signing Certificates do not identify a particular software object, identifying only the publisher of software.

1.2 Document name and identification

The following Certificate Policy Identifier is reserved for use by CAs as a required means of asserting compliance with these Requirements for Non-EV Code Signing Certificates:

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(4) code signing(1)} (2.23.140.1.4.1).`

The following Certificate Policy Identifier is reserved for use by CAs as a required means of asserting compliance with these Requirements for EV Code Signing Certificates follows:

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(3)}(2.23.140.1.3).`

The following Certificate Policy Identifier is reserved for use by CAs as a required means of asserting compliance with these Requirements for Timestamp Certificates:

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(4) timestamping(2)} (2.23.140.1.4.2).`

1.2.1 Revisions

Ver.	Ballot	Description	Effective
1.2	CSC-1	Adopt Baseline Requirements version 1.2	13 Aug 2019
2.0	CSC-2	Adopt combined EV and BR Code Signing Document	2 Sept 2020

Ver.	Ballot	Description	Effective
2.1	CSC-4	Move deadline for transition to RSA-3072 and SHA-2 timestamp tokens	7 Nov 2020
2.2	CSC-7	Update to merge EV and non-EV clauses	8 March 2021
2.3	CSC-8	Update to Revocation response mechanisms. key protection for EV certificates, and clean-up of 11.2.1 & Appendix B	2 May 2021
2.4	CSC-9	Spring 2021 Clean-up and Clarification	8 September 2021
2.5	CSC-10	WebTrust CSBR v2.0 Audit Criteria	12 September 2021
2.6	CSC-11	Update to log data retention requirements	3 November 2021
2.7	CSC-12	CRL Revocation Date Clarification	3 December 2021
2.8	CSC-13	Update to Subscriber Key Protection Requirements	6 May 2022
3.0	CSC-14	Convert Code Signing Baseline Requirements to RFC 3647 Framework	29 June 2022
3.1	CSC-15	Summer 2022 Clean-up	19 September 2022
3.2	CSC-17	Subscriber Private Key Protection Extension	28 October 2022
3.3	CSC-18	Update Revocation Requirements	29 June 2023
3.4	CSC-19	Remove SSL BR References	5 September 2023
3.5	CSC-20	Restore Version Reference to EV Guidelines	7 December 2023
3.6	CSC-21	Improved signing services requirements	28 February 2024
3.7	CSC-22	High risk changes	28 February 2024

1.2.2 Relevant Dates

Compliance	Section(s)	Summary Description (See Full Text for Details)
2021-06-01	6.1.5	CAs SHALL support minimum RSA-3072 for Code Signing Certificates, Root Certificates and Subordinate CA Certificates. CAs SHALL NOT support SHA-1 digest algorithm for Code Signing Certificates.
2021-06-01	5.3	After 2021-06-01, the CA shall meet the requirements of EV Guidelines Section 14.1 for Non-EV and EV Code Signing Certificates.
2021-06-01	6.2.7.4	For EV Code Signing Certificates, Signing Services shall protect Private Keys in a FIPS 140-2 level 2 (or equivalent) crypto module. After 2021-06-01, the same protection requirements SHALL apply to Non EV Code Signing Certificates.

Compliance	Section(s)	Summary Description (See Full Text for Details)
2021-11-01	3.2.2.1 (5)	The method used to verify the identity of the Certificate Requester SHALL be per section 3.2.3.
2022-03-31	7.1.6.3	Subordinate CA Certificates issued for Subordinate CA that issues Timestamp Certificates and is an Affiliate of the Issuing CA must include the reserved identifier specified in Section 7.1.6.1.
2022-04-30	7.1.3.2.1	CAs SHALL NOT support SHA-1 digest algorithm for Timestamp tokens.
2022-07-01	7.2.2	For Code Signing Certificates, the time encoded in the Invalidity Date CRL entry extension MUST be equal to the time encoded in the revocationDate field of the CRL entry.
2023-06-01	6.2.7.4.2	Effective June 1, 2023, for Code Signing Certificates, CAs SHALL ensure that the Subscriber's Private Key is generated, stored, and used in a suitable Hardware Crypto Module that meets or exceeds the requirements specified in section 6.2.7.4.1 (7-9).
2023-06-01	6.2.7.4.2	Effective June 1, 2023, for Code Signing Certificates, CAs SHALL ensure that the Subscriber's Private Key is generated, stored, and used in a suitable Hardware Crypto Module that meets or exceeds the requirements specified in section 6.2.7.4.1 using one of the methods in 6.2.7.4.2.
2023-06-01	6.2.7.4.2	Any other method the CA uses to satisfy the Subscriber's compliance with the private key protection requirements. The CA SHALL specify and describe in detail those other methods in its Certificate Policy or Certification Practice Statement, and SHALL propose those methods to the CA/Browser Forum Code Signing Working Group for inclusion into these requirements until June 1, 2023, using the questions@cabforum.org mailing list. After that date, the Code Signing Working Group will discuss the removal of this "any other method" and allow only CA/Browser Forum approved methods.
2024-04-15	4.9.1	This ballot updates the "Circumstances for revocation" in order to align it with the TLS and S/MIME BRs and set stricter requirements for revocation due to Private Key Compromise and use in Suspect Code.
2024-06-15	8.4.2	For Audit Periods starting after June 30, 2024, the Signing Service MUST undergo a conformity assessment audit for compliance with these Requirements performed in accordance with one of the schemes specified in Section 8.4.2.
2025-03-15	3.2.10	Prior to the use of an Incorporating Agency or Registration Agency to fulfill these verification requirements, the CA MUST publicly disclose Agency Information about the Incorporating Agency or Registration Agency.

1.3 PKI participants

1.3.1 Certification authorities

1.3.2 Registration authorities

Except as stated in Section 8 (5), the CA MAY delegate the performance of all, or any part, of these Requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of this document.

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

1. Meet the qualification requirements of Section 5.3 when applicable to the delegated function,
2. Retain documentation in accordance with Section 5.4.1,

3. Abide by the other provisions of these Requirements that are applicable to the delegated function, and
4. Comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.

The CA MUST verify that any Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3 of this document and the document retention and event logging requirements of Section 5.4 of this document.

1.3.2.1 Delegation of Functions to Registration Authorities and Subcontractors

1.3.2.1.1 General

The CA MAY delegate the performance of all or any part of a requirement of these Requirements to an Affiliate or a Registration Authority (RA) or subcontractor, provided that the process employed by the CA fulfills all of the requirements of Section 3.2.9. Affiliates and/or RAs must comply with the qualification requirements of Section 5.3.

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 and the document retention and event logging requirements of Section 5.4.

1.3.2.1.2 Enterprise RAs

The CA MAY contractually authorize a Subscriber to perform the RA function and authorize the CA to issue additional EV Code Signing Certificates. In such case, the Subscriber SHALL be considered an Enterprise RA, and the following requirements SHALL apply:

1. In all cases, the Subscriber MUST be an organization verified by the CA in accordance with these Requirements;
2. The CA MUST impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by the Enterprise RA; and
3. The Final Cross-Correlation and Due Diligence requirements of Section 3.2.9 MAY be performed by a single person representing the Enterprise RA.

Enterprise RAs that authorize the issuance of EV Code Signing Certificates solely for its own organization are exempted from the audit requirements of Section 8.4. In all other cases, the requirements of Section 8.4 SHALL apply.

1.3.2.1.3 Guidelines Compliance Obligation

In all cases, the CA MUST contractually obligate each Affiliate, RA, subcontractor, and Enterprise RA to comply with all applicable requirements in these Requirements and to perform them as required of the CA itself. The CA SHALL enforce these obligations and internally audit each Affiliate's, RA's, subcontractor's, and Enterprise RA's compliance with these Requirements on an annual basis.

1.3.2.1.4 Allocation of Liability

As specified in Section 9.8.

1.3.3 Subscribers

1.3.4 Relying parties

1.3.5 Other participants

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

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

1.4 Certificate usage

1.4.1 Appropriate certificate uses

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

1.4.2 Prohibited certificate uses

No stipulation.

1.5 Policy administration

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

1.5.1 Organization administering the document

No stipulation.

1.5.2 Contact person

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

1.5.3 Person determining CPS suitability for the policy

No stipulation.

1.5.4 CPS approval procedures

No stipulation.

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

Capitalized Terms are as defined below and in the EV SSL Guidelines:

Accounting Practitioner: A certified public accountant, chartered accountant, or a person with an equivalent license within the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility; provided that an accounting standards body in the jurisdiction maintains full (not "suspended" or "associate") membership status with the International Federation of Accountants.

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, and/or 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.

Anti-Malware Organization: An entity that maintains information about Suspect Code and/or develops software used to prevent, detect, or remove malware.

Application Software Supplier: A supplier of software or other relying-party application software that displays or uses Code Signing Certificates, incorporates Root Certificates, and adopts these Requirements as all or part of its requirements for participation in a root store program.

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

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

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

Baseline Requirements: The Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates as published by the CA/Browser Forum.

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

partnerships, unincorporated associations, sole proprietorships, etc.

Certificate Approver: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to

1. act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and
2. to approve EV Code Signing Certificate Requests submitted by other Certificate Requesters.

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

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

Confirming Person: A position within an Applicant's organization that confirms the particular fact at issue.

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

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

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

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

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

Certificate Beneficiaries: All Application Software Suppliers with whom the CA or its Root CA has entered into a contract for distribution of its Root Certificate in software distributed by such Application Software Suppliers and all Relying Parties who reasonably rely on such a Certificate while a Code Signature associated with the Certificate is valid.

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

Certificate Policy Identifier: As described in Section 7.1.6

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.

Certification Authority: An organization subject to these Requirements that is responsible for a Code Signing Certificate and, under these Requirements, oversees the creation, issuance, revocation, and management of Code Signing Certificates. Where the CA is also the Root CA, references to the CA are synonymous with Root CA.

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

Certificate Requester: A natural person who is the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or the employee or agent of a third party (such as software publisher) who completes and submits a Certificate Request on behalf of the Applicant.

Code: A contiguous set of bits that has been or can be digitally signed with a Private Key that corresponds to a Code Signing Certificate.

Code Signature: A Signature logically associated with a signed Code.

Code Signing Certificate: A digital certificate issued by a CA that contains a Code Signing EKU.

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

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

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

CSPRNG: A random number generator intended for use in 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.

Declaration of Identity: A written document that consists of the following:

1. the identity of the person performing the verification,
2. a signature of the Applicant,
3. a unique identifying number from an identification document of the Applicant,
4. the date of the verification, and
5. a signature of the Verifying Person.

Demand Deposit Account: A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as a share draft account, a current account, or a checking account.

EV Authority: A source other than the Certificate Approver, through which verification occurs that the Certificate Approver is expressly authorized by the Applicant, as of the date of the EV Code Signing Certificate Request, to take the Request actions described in these Guidelines.

EV Code Signing Certificate Request: A request from an Applicant to the CA requesting that the CA issue an EV Code Signing Certificate to the Applicant, which request is validly authorized by the Applicant and signed by the Applicant Representative.

EV Code Signing Certificate: A Code Signing Certificate that contains subject information specified in these Guidelines for Extended Validation and that has been validated in accordance with these Guidelines for Extended Validation.

EV Processes: The keys, software, processes, and procedures by which the CA verifies Certificate Data under the EV Code Signing Certificate policy, issues EV Code Signing Certificates, maintains a Repository, and revokes EV Code Signing Certificates.

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

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

Guidelines: This document.

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

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

High Risk Region of Concern (HRRC): As set forth in Appendix A, a geographic location where the detected number of Code Signing Certificates associated with signed Suspect Code exceeds 5% of the total number of detected Code Signing Certificates originating or associated with the same geographic area.

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

Independent Confirmation From Applicant: Confirmation of a particular fact received by the CA pursuant to the provisions of the Guidelines or binding upon the Applicant.

Individual: A natural person.

Individual Applicant: An Applicant who is a natural person and requests a Certificate that will list the Applicant's legal name as the Certificate's Subject.

International Organization: An organization founded by a constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments.

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

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

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

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

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

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

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system. In the EV context, it is a Private Organization, Government Entity, Business Entity, or Non-Commercial Entity.

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

Legal Practitioner: A person who is either a lawyer or a Latin Notary as described in these Guidelines and competent to render an opinion on factual claims of the Applicant.

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

Non-EV Code Signing Certificate: Term used to signify requirements that are applicable to Code Signing Certificates which do not have to meet the EV requirements.

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

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

OCSP 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.

Organizational Applicant: An Applicant that requests a Certificate with a name in the Subject field that is for an organization and not the name of an individual. Organizational Applicants include private and public corporations, LLCs, partnerships, government entities, non-profit organizations, trade associations, and other legal entities.

Parent Company: A company that Controls a Subsidiary Company.

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

Platform: The computing environment in which an Application Software Supplier uses Code Signing Certificates, incorporates Root Certificates, and adopts these Requirements.

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

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.

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

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

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

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

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

Qualified Government Information Source: A database maintained by a Government Entity (e.g. SEC filings) that meets the requirements of Section 3.2.2.2.10.6.

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

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

Registration Agency: A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited to

1. a State Department of Corporations or a Secretary of State;
2. a licensing agency, such as a State Department of Insurance; or
3. a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Office of the Comptroller of the Currency or Office of Thrift Supervision.

Registration Authority (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 Identifier: The unique code assigned to an Applicant by the Incorporating or Registration Agency in such entity's Jurisdiction of Incorporation or Registration.

Registered Agent: An individual or entity that is:

1. authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and
2. listed in the official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in (i) above.

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 Baseline Requirements found in this document.

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

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

Signature: An encrypted electronic data file which is attached to or logically associated with other electronic data and which (i) identifies and is uniquely linked to the signatory of the electronic data, (ii) is created using means that the signatory can maintain under its sole control, and (iii) is

linked in a way so as to make any subsequent changes that have been made to the electronic data detectable.

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

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

Subject: The Subject of a Code Signing Certificate is the entity responsible for distributing the software but does not necessarily hold the copyright to the Code.

Subject Identity Information: Information that identifies the Certificate Subject.

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 Code Signing 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.

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

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

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.

Timestamp Authority: A service operated by the CA or a delegated third party for its own code signing certificate users that timestamps data using a certificate chained to a public root, thereby asserting that the data (or the data from which the data were derived via a secure hashing algorithm) existed at the specified time.

Timestamp Certificate: A certificate issued to a Timestamp Authority to use to timestamp data.

Trusted Platform Module: A microcontroller that stores keys, passwords and digital certificates, usually affixed to the motherboard of a computer, which due to its physical nature makes the information stored there more secure against external software attack or physical theft.

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

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

Validity Period: The validity period is as defined within RFC 5280, Section 4.1.2.5: the period of time from notBefore through notAfter, inclusive.

Verifying Person: A notary, attorney, Latin notary, accountant, individual designated by a government agency as authorized to verify identities, or agent of the CA, who attests to the identity of an individual.

1.6.2 Abbreviations and Acronyms

Acronym	Meaning
BIPM	International Bureau of Weights and Measures
BIS	(US Government) Bureau of Industry and Security
CA	Certification Authority
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPA	Chartered Professional Accountant
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSO	Chief Security Officer
DBA	Doing Business As
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
IFAC	International Federation of Accountants
IRS	Internal Revenue Service
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
QGIS	Qualified Government Information Source
QTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority
SEC	(US Government) Securities and Exchange Commission
UTC(k)	National realization of Coordinated Universal Time

1.6.3 References

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

Providers

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

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

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

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

Guidelines for the Issuance and Management of Extended Validation Certificates, Version 1.7.2, available at https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.7.2.pdf.

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

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

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf.

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

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.

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

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

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

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

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

WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements, available at https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria.

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

1.6.4 Conventions

Terms not otherwise defined in these Requirements are as defined in the CA's applicable agreements, user manuals, Certificate Policies, and Certification Practice Statements.

The key words "MUST","MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements are used in accordance with RFC 2119.

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

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

2.1 Repositories

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

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

2.2 Publication of certification information

The CA and its Root CA MUST develop, implement, enforce, display prominently on its web site, and periodically update its policies and practices, including its Certificate Policy and/or Certification Practice Statement, that implement the most current version of these Requirements. The Certificate Policy and/or Certification Practice Statement MUST specify the CA's (and applicable Root CA's) entire root certificate hierarchy including all roots that its Code Signing Certificates depend on for proof of those Code Signing Certificates' authenticity.

Each CA MUST represent that it has disclosed all Cross Certificates in its Certificate Policy/Certificate Practice Statement 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).

Each CA, including Root CAs, MUST publicly disclose their policies and practices through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA MUST publicly disclose its Certificate Practice Statement and/or Certificate Policies and structure the disclosures in accordance with RFC 3647.

Each CA MUST give public effect to these Requirements and represent that they will adhere to the latest published version by either (i) incorporating the Requirements directly into their respective Certification Practice Statements or (ii) by referencing the Requirements using a clause such as the following:

> [Name of CA] conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at [URL]. If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

In either case, each CA MUST include a link to the official version of these Requirements. In addition, each CA MUST include (directly or by reference) applicable parts of these Requirements in all contracts with Subordinate CAs, RAs, Signing Services and subcontractors, that involve or relate to the issuance or management of Certificates. CAs MUST enforce compliance with such terms.

2.3 Time or frequency of publication

The CA SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. The CA SHALL indicate conformance with this requirement by incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

2.4 Access controls on repositories

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

3.1.2 Need for names to be meaningful

3.1.3 Anonymity or pseudonymity of subscribers

3.1.4 Rules for interpreting various name forms

3.1.5 Uniqueness of names

3.1.6 Recognition, authentication, and role of trademarks

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

3.2.2 Authentication of organization identity

The CA SHALL verify the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of Section 3.2.2.1 or Section 3.2.2.2 and that is described in the CA's Certificate Policy and/or Certification Practice Statement. The CA SHALL inspect any document relied upon under this Section for alteration or falsification.

3.2.2.1 Authentication of organization identity for Non-EV Code Signing Certificates

Prior to issuing a Code Signing Certificate to an Organizational Applicant, the CA MUST:

1. Verify the Subject's legal identity, including any DBA proposed for inclusion in a Certificate, in accordance with Section 3.2.2.1.1 and Section 3.2.2.1.2. The CA MUST also obtain, whenever available, a specific Registration Identifier assigned to the Applicant by a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition,
2. Verify the Subject's address in accordance with Section 3.2.2.1.1,
3. Verify the Certificate Requester's authority to request a Code Signing Certificate and the authenticity of the Certificate Request using a Reliable Method of Communication in accordance with Section 3.2.5, and
4. If the Subject's or Subject's Affiliate's, Parent Company's, or Subsidiary Company's date of formation, as indicated by either a QIIS or QGIS, was less than three years prior to the date of the Certificate Request, verify the identity of the Certificate Requester. Effective 1 November 2021, the method used to verify the identity of the Certificate Requester SHALL be per Section 3.2.3.1.

3.2.2.1.1 Identity

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

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

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

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

3.2.2.1.2 DBA/Tradename

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

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

3.2.2.2 Authentication of organization identity for EV Code Signing Certificates

Before issuing a EV Code Signing Certificate, the CA MUST ensure that all Subject organization information to be included in the EV Code Signing Certificate conforms to the requirements of, and is verified in accordance with this section and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended to accomplish the following:

1. Verify Applicant's existence and identity, including;
    1. Verify the Applicant's legal existence and identity (as more fully set forth in Section 3.2.2.2.1 herein),
    2. Verify the Applicant's physical existence (business presence at a physical address), and
    3. Verify the Applicant's operational existence (business activity).
2. Verify the Applicant's authorization for the EV Code Signing Certificate, including;
    1. Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
    2. Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and
    3. Verify that a Certificate Approver has signed or otherwise approved the EV Code Signing Certificate Request.

As a general rule, the CA is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in the subsections below. The Acceptable Methods of Verification are set forth below. In all cases, however, the CA is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to

satisfy the applicable Verification Requirement.

The following Applicant roles are required for the issuance of an EV Code Signing Certificate.

1. **Certificate Requester**: The EV Code Signing Certificate Request MUST be submitted by an authorized Certificate Requester. A Certificate Requester is a natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Code Signing Certificate Request on behalf of the Applicant.
2. **Certificate Approver**: The EV Code Signing Certificate Request MUST be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to
    1. act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and
    2. to approve EV Code Signing Certificate Requests submitted by other Certificate Requesters.
3. **Contract Signer**: A Subscriber Agreement applicable to the requested EV Code Signing Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.
4. **Applicant Representative**: In the case where the CA and the Subscriber are affiliated, Terms of Use applicable to the requested EV Code Signing Certificate MUST be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.

The Applicant MAY authorize one individual to occupy two or more of these roles. The Applicant MAY authorize more than one individual to occupy any of these roles.

3.2.2.2.1 Verification of Applicant's Legal Existence and Identity

3.2.2.2.1.1 Verification Requirements

To verify the Applicant's legal existence and identity, the CA MUST do the following.

1. **Private Organization Subjects**
    1. **Legal Existence**: Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating or Registration Agency by labels such as "inactive", "invalid", "not current", or the equivalent.
    2. **Organization Name**: Verify that the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration matches the Applicant's name in the EV Code Signing Certificate Request.
    3. **Registration Number**: Obtain the specific Registration Number assigned to the Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of

Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Incorporation or Registration.

4. **Registered Agent**: Obtain the identity and address of the Applicant's Registered Agent or Registered Office (as applicable in the Applicant's Jurisdiction of Incorporation or Registration).

2. **Government Entity Subjects**

    1. **Legal Existence**: Verify that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.
    2. **Entity Name**: Verify that the Applicant's formal legal name matches the Applicant's name in the EV Code Signing Certificate Request.
    3. **Registration Number**: The CA MUST attempt to obtain the Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is a Government Entity.

3. **Business Entity Subjects**

    1. **Legal Existence**: Verify that the Applicant is engaged in business under the name submitted by the Applicant in the Application.
    2. **Organization Name**: Verify that the Applicant's formal legal name as recognized by the Registration Agency in the Applicant's Jurisdiction of Registration matches the Applicant's name in the EV Code Signing Certificate Request.
    3. **Registration Number**: Attempt to obtain the specific unique Registration Number assigned to the Applicant by the Registration Agency in the Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Registration.
    4. **Principal Individual**: Verify the identity of the identified Principal Individual.

4. **Non-Commercial Entity Subjects (International Organizations)**

    1. **Legal Existence**: Verify that the Applicant is a legally recognized International Organization Entity.
    2. **Entity Name**: Verify that the Applicant's formal legal name matches the Applicant's name in the EV Code Signing Certificate Request.
    3. **Registration Number**: The CA MUST attempt to obtain the Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is an International Organization Entity.

3.2.2.2.1.2 Acceptable Method of Verification

1. **Private Organization Subjects**: Unless verified under subsection (6), all items listed in Section 3.2.2.2.1.1 (1) MUST be verified directly with, or obtained directly from, the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Such verification MAY be through use of a Qualified Government Information Source operated by, or on behalf of, the Incorporating or Registration Agency, or by direct contact with the Incorporating or Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the

Qualified Government Information Source, Incorporating or Registration Agency, or from a Qualified Independent Information Source.

2. **Government Entity Subjects**: Unless verified under subsection (6), all items listed in Section 3.2.2.2.1.1 (2) MUST either be verified directly with, or obtained directly from, one of the following:

    1. a Qualified Government Information Source in the political subdivision in which such Government Entity operates;
    2. a superior governing Government Entity in the same political subdivision as the Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department), or
    3. from a judge that is an active member of the federal, state or local judiciary within that political subdivision.

    Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an Attorney as set forth in Section 3.2.2.2.10.1.

    Such verification MAY be by direct contact with the appropriate Government Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.

3. **Business Entity Subjects**: Unless verified under subsection (6), items listed in Section 3.2.2.2.1.1 (3) (i) through (iii) above, MUST be verified directly with, or obtained directly from, the Registration Agency in the Applicant's Jurisdiction of Registration. Such verification MAY be performed by means of a Qualified Government Information Source, a Qualified Governmental Tax Information Source, or by direct contact with the Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Qualified Governmental Tax Information Source or Registration Agency, or from a Qualified Independent Information Source. In addition, the CA MUST validate a Principal Individual associated with the Business Entity pursuant to the requirements in subsection (4), below.

4. **Principal Individual**: A Principal Individual associated with the Business Entity MUST be validated in a face-to-face setting. The CA MAY rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that the CA has evaluated the validation procedure and concluded that it satisfies the requirements of the Guidelines for face-to-face validation procedures. Where no face-to-face validation was conducted by the Registration Agency, or the Registration Agency's face-to-face validation procedure does not satisfy the requirements of the Guidelines, the CA SHALL perform face-to-face validation.

    1. **Face-To-Face Validation**: The face-to-face validation MUST be conducted before either an employee of the CA, a Latin Notary, a Notary (or equivalent in the Applicant's jurisdiction), a Lawyer, or Accountant (Third-Party Validator). The Principal Individual(s) MUST present the following documentation (Vetting Documents) directly to the Third-Party Validator:

        1. A Personal Statement that includes the following information:

            1. Full name or names by which a person is, or has been, known (including all other names used);
            2. Residential Address at which he/she can be located;

3. Date of birth; and
4. An affirmation that all of the information contained in the Certificate Request is true and correct.

2. A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:
    1. A passport;
    2. A driver's license;
    3. A personal identification card;
    4. A concealed weapons permit; or
    5. A military ID.
3. At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which MUST be from a financial institution.
    1. Acceptable financial institution documents include:
        1. A major credit card, provided that it contains an expiration date and it has not expired'
        2. A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired,
        3. A mortgage statement from a recognizable lender that is less than six months old,
        4. A bank statement from a regulated financial institution that is less than six months old.
    2. Acceptable non-financial documents include:
        1. Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill),
        2. A copy of a statement for payment of a lease, provided that the statement is dated within the past six months,
        3. A certified copy of a birth certificate,
        4. A local authority tax bill for the current year,
        5. A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.

The Third-Party Validator performing the face-to-face validation MUST:

1. Attest to the signing of the Personal Statement and the identity of the signer; and
2. Identify the original Vetting Documents used to perform the identification. In addition, the Third-Party Validator MUST attest on a copy of the current signed government-issued photo identification document that it is a full, true, and accurate reproduction of the original.

2. **Verification of Third-Party Validator**: The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), lawyer, or accountant in the jurisdiction of the Individual's residency, and that the Third-Party Validator actually did perform the services and did attest to the signature of the Individual.

3. **Cross-checking of Information**: The CA MUST obtain the signed and attested Personal Statement together with the attested copy of the current signed government-issued photo identification document. The CA MUST review the documentation to determine that the information is consistent, matches the information in the application, and identifies the Individual. The CA MAY rely on electronic copies of this documentation, provided that:

    1. the CA confirms their authenticity (not improperly modified when compared with the underlying original) with the Third-Party Validator; and
    2. electronic copies of similar kinds of documents are recognized as legal substitutes for originals under the laws of the CA's jurisdiction.

5. **Non-Commercial Entity Subjects (International Organization)**: Unless verified under subsection (6), all items listed in Section 3.2.2.2.1.1 (4) MUST be verified either:

    1. With reference to the constituent document under which the International Organization was formed; or
    2. Directly with a signatory country's government in which the CA is permitted to do business. Such verification may be obtained from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or
    3. Directly against any current list of qualified entities that the CA/Browser Forum may maintain at www.cabforum.org.
    4. In cases where the International Organization applying for the EV Code Signing Certificate is an organ or agency - including a non-governmental organization of a verified International Organization, then the CA may verify the International Organization Applicant directly with the verified umbrella International Organization of which the Applicant is an organ or agency.

6. The CA may rely on a Verified Professional Letter to establish the Applicant's information listed in (1)-(5) above if:

    1. the Verified Professional Letter 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
    2. the CA confirms the Applicant's organization name specified in the Verified Professional Letter with a QIIS or QGIS.

3.2.2.2.2 Verification of Applicant's Legal Existence and Identity – Assumed Name

1. **Verification Requirements**: If, in addition to the Applicant's formal legal name, as recorded with the applicable Incorporating Agency or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, the Applicant's identity, as asserted in the EV Code Signing Certificate, is to contain any assumed name (also known as "doing business as", "DBA", or "d/b/a" in the US, and "trading as" in the UK) under which the Applicant conducts business, the CA MUST 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 Place of Business (as verified in accordance with these Guidelines), and
    2. that such filing continues to be valid.

2. **Acceptable Method of Verification**: To verify any assumed name under which the Applicant conducts business:

    1. The CA MAY verify the assumed name through use of a Qualified Government Information Source operated by, or on behalf of, an appropriate government agency in the jurisdiction of the Applicant's Place of Business, or by direct contact with such government agency in person or via mail, e-mail, Web address, or telephone; or
    2. The CA MAY verify the assumed name through use of a Qualified Independent Information Source provided that the QIIS has verified the assumed name with the appropriate government agency.
    3. The CA MAY rely on a Verified Professional Letter 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.

3.2.2.2.3 Verification of Applicant's Physical Existence

3.2.2.2.3.1. Address of Applicant's Place of Business

1. **Verification Requirements**: To verify the Applicant's physical existence and business presence, the CA MUST verify that the physical address provided by the Applicant is an address where the Applicant or a Parent/Subsidiary Company conducts business operations (not, for example, a mail drop or P.O. box, or 'care of' (C/O) address, such as an address for an agent of the Organization), and is the address of the Applicant's Place of Business.
2. **Acceptable Methods of Verification**
    1. **Place of Business in the Country of Incorporation or Registration**
        1. For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and whose Place of Business is NOT the same as that indicated in the relevant Qualified Government Information Source used in Section 3.2.2.2.1 to verify legal existence:
            1. For Applicants listed at the same Place of Business address in the current version of either at least one QGIS (other than that used to verify legal existence), QIIS or QTIS, the CA MUST confirm that the Applicant's address, as listed in the EV Code Signing Certificate Request, is a valid business address for the Applicant or a Parent/Subsidiary Company by reference to such QGIS, QIIS, or QTIS, and MAY rely on the Applicant's representation that such address is its Place of Business;
            2. For Applicants who are not listed at the same Place of Business address in the current version of either at least one QIIS or QTIS, the CA MUST confirm that the address provided by the Applicant in the EV Code Signing Certificate Request is the Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to the business address, which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:
                1. Verify that the Applicant's business is located at the exact address stated in the EV Code Signing Certificate Request (e.g., via permanent signage, employee confirmation, etc.),
                2. Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location,
                3. Indicate whether there is a permanent sign (that cannot be moved) that

identifies the Applicant,
4. Indicate whether there is evidence that the Applicant is conducting ongoing business activities at the site (not that it is just, for example, a mail drop, P.O. box, etc.), and
5. Include one or more photos of
    1. the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and
    2. the interior reception area or workspace.

2. For all Applicants, the CA MAY alternatively rely on a Verified Professional Letter that indicates the address of the Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.
3. For Government Entity Applicants, the CA MAY rely on the address contained in the records of the QGIS in the Applicant's jurisdiction.
4. For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and where the QGIS used in Section 3.2.2.2.1 to verify legal existence contains a business address for the Applicant, the CA MAY rely on the address in the QGIS to confirm the Applicant's or a Parent/Subsidiary Company's address as listed in the EV Code Signing Certificate Request, and MAY rely on the Applicant's representation that such address is its Place of Business.

2. **Place of Business not in the Country of Incorporation or Registration**: The CA MUST rely on a Verified Professional Letter that indicates the address of the Applicant's Place of Business and that business operations are conducted there.

3.2.2.2.4 Verified Method of Communication

1. **Verification Requirements**: To assist in communicating with the Applicant and confirming that the Applicant is aware of and approves issuance, the CA MUST verify a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant.
2. **Acceptable Methods of Verification**: To verify a Verified Method of Communication with the Applicant, the CA MUST:
    1. Verify that the Verified Method of Communication belongs to the Applicant, or a Parent/Subsidiary or Affiliate of the Applicant, by matching it with one of the Applicant's Parent/Subsidiary or Affiliate's Places of Business in:
        1. records provided by the applicable phone company;
        2. a QGIS, QTIS, or QIIS; or
        3. a Verified Professional Letter; and
    2. Confirm the Verified Method of Communication by using it to obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant, or a Parent/Subsidiary or Affiliate of Applicant, can be contacted reliably by using the Verified Method of Communication.

3.2.2.2.5 Verification of Applicant's Operational Existence

1. **Verification Requirements**: The CA MUST verify that the Applicant has the ability to engage in business by verifying the Applicant's, or Affiliate/Parent/Subsidiary Company's, operational existence. The CA MAY rely on its verification of a Government Entity's legal existence under Section 3.2.2.2.1 as verification of a Government Entity's operational

existence.

2. **Acceptable Methods of Verification**: To verify the Applicant's ability to engage in business, the CA MUST verify the operational existence of the Applicant, or its Affiliate/Parent/Subsidiary Company, by:
    1. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency;
    2. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current QIIS or QTIS;
    3. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution; or
    4. Relying on a Verified Professional Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

3.2.2.2.6 Verification of Applicant's Domain Name

Code Signing Certificates SHALL NOT include a Domain Name.

3.2.2.2.7 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

1. **Verification Requirements**: For both the Contract Signer and the Certificate Approver, the CA MUST verify the following.
    1. **Name, Title and Agency**: The CA MUST verify the name and title of the Contract Signer and the Certificate Approver, as applicable. The CA MUST also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.
    2. **Signing Authority of Contract Signer**: The CA MUST verify that the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.
    3. **EV Authority of Certificate Approver**: The CA MUST verify, through a source other than the Certificate Approver him- or herself, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Code Signing Certificate Request:
        1. Submit, and, if applicable, authorize a Certificate Requester to submit, the EV Code Signing Certificate Request on behalf of the Applicant; and
        2. Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV Code SigningCertificate; and
        3. Approve EV Code Signing Certificate Requests submitted by a Certificate Requester.

2. **Acceptable Methods of Verification – Name, Title and Agency**: Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include the following.
    1. **Name and Title**: The CA MAY verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable assurance that a person claiming to act in such a role is in fact the named person

designated to act in such role.

2. **Agency**: The CA MAY verify the agency of the Contract Signer and the Certificate Approver by:
    1. Contacting the Applicant using a Verified Method of Communication for the Applicant, and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee;
    2. Obtaining an Independent Confirmation From the Applicant (as described in Section 3.2.2.2.12), or a Verified Professional Letter verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has otherwise been appointed as an agent of the Applicant; or
    3. Obtaining confirmation from a QIIS or QGIS that the Contract Signer and/or Certificate Approver is an employee of the Applicant.

The CA MAY also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between the CA and the Applicant signed by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified.

3. **Acceptable Methods of Verification – Authority**: Acceptable methods of verification of the Signing Authority of the Contract Signer, and the EV Authority of the Certificate Approver, as applicable, include:

    1. **Verified Professional Letter**: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a Verified Professional Letter;
    2. **Corporate Resolution**: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is
        1. certified by the appropriate corporate officer (e.g., secretary), and
        2. the CA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification;
    3. **Independent Confirmation from Applicant**: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by obtaining an Independent Confirmation from the Applicant (as described in Section 3.2.2.2.12);
    4. **Contract between CA and Applicant**: The EV Authority of the Certificate Approver MAY be verified by reliance on a contract between the CA and the Applicant that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;
    5. **Prior Equivalent Authority**: The signing authority of the Contract Signer, and/or the EV authority of the Certificate Approver, MAY be verified by relying on a demonstration of Prior Equivalent Authority.
        1. Prior Equivalent Authority of a Contract Signer MAY be relied upon for confirmation or verification of the signing authority of the Contract Signer when the Contract Signer has executed a binding contract between the CA and the Applicant with a legally valid and enforceable seal or handwritten signature and only when the contract was executed more than 90 days prior to the EV Code Signing Certificate application. The CA MUST record sufficient details of the previous agreement to correctly identify it and associate it with the EV application.

Such details MAY include any of the following:

1. Agreement title,
2. Date of Contract Signer's signature,
3. Contract reference number, and
4. Filing location.

2. Prior Equivalent Authority of a Certificate Approver MAY be relied upon for confirmation or verification of the EV Authority of the Certificate Approver when the Certificate Approver has performed one or more of the following:
   1. Under contract to the CA, has served (or is serving) as an Enterprise RA for the Applicant, or
   2. Has participated in the approval of one or more certificate requests, for certificates issued by the CA and which are currently and verifiably in use by the Applicant. In this case the CA MUST have contacted the Certificate Approver by phone at a previously validated phone number or have accepted a signed and notarized letter approving the certificate request.

6. **QIIS or QGIS**: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by a QIIS or QGIS that identifies the Contract Signer and/or the Certificate Approver as a corporate officer, sole proprietor, or other senior official of the Applicant.
7. **Contract Signer's Representation/Warranty**: Provided that the CA verifies that the Contract Signer is an employee or agent of the Applicant, the CA MAY rely on the signing authority of the Contract Signer by obtaining a duly executed representation or warranty from the Contract Signer that includes the following acknowledgments:
   1. That the Applicant authorizes the Contract Signer to sign the Subscriber Agreement on the Applicant's behalf,
   2. That the Subscriber Agreement is a legally valid and enforceable agreement,
   3. That, upon execution of the Subscriber Agreement, the Applicant will be bound by all of its terms and conditions,
   4. That serious consequences attach to the misuse of an EV Code Signing Certificate, and
   5. The contract signer has the authority to obtain the digital equivalent of a corporate seal, stamp or officer's signature to establish the authenticity of the company's Web site.

Note: An example of an acceptable representation/warranty appears in Appendix E.

4. **Pre-Authorized Certificate Approver**: Where the CA and Applicant contemplate the submission of multiple future EV Code Signing Certificate Requests, then, after the CA:

   1. Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant; and
   2. Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in 3.2.2.2.7 (3) Acceptable Methods of Verification – Authority.

   The CA and the Applicant MAY enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise EV Authority with respect to each future EV Code Signing Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

Such an agreement MUST provide that the Applicant shall be obligated under the Subscriber Agreement for all EV Code Signing Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and MUST include mutually agreed-upon provisions for:

1. authenticating the Certificate Approver when EV Code Signing Certificate Requests are approved,
2. periodic re-confirmation of the EV Authority of the Certificate Approver,
3. secure procedures by which the Applicant can notify the CA that the EV Authority of any such Certificate Approver is revoked, and
4. such other appropriate precautions as are reasonably necessary.

3.2.2.2.8 Verification of Signature on Subscriber Agreement and EV Code Signing Certificate Requests

Both the Subscriber Agreement and each non-pre-authorized EV Code Signing Certificate Request MUST be signed. The Subscriber Agreement MUST be signed by an authorized Contract Signer. The EV Code Signing Certificate Request MUST be signed by the Certificate Requester submitting the document, unless the Certificate Request has been pre-authorized in line with Section 3.2.2.2.7 (4) (pre-Authorized Certificate Approver). If the Certificate Requester is not also an authorized Certificate Approver, then an authorized Certificate Approver MUST independently approve the EV Code Signing Certificate Request. In all cases, applicable signatures MUST be a legally valid and contain an enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Code Signing Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Code Signing Certificate Request), that binds the Applicant to the terms of each respective document.

1. **Verification Requirements**:
    1. **Signature**: The CA MUST authenticate the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each EV Code Signing Certificate Request in a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.
    2. **Approval Alternative**: In cases where an EV Code Signing Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the EV Code Signing Certificate Request by a Certificate Approver in accordance with the requirements of Section 3.2.2.2.9 can substitute for authentication of the signature of the Certificate Requester on such EV Code Signing Certificate Request.
2. **Acceptable Methods of Signature Verification**: Acceptable methods of authenticating the signature of the Certificate Requester or Contract Signer include the following:
    1. Contacting the Applicant using a Verified Method of Communication for the Applicant, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;
    2. A letter mailed to the Applicant's or Agent's address, as verified through independent means in accordance with these Guidelines, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response through a Verified Method of Communication from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;
    3. Use of a signature process that establishes the name and title of the signer in a secure

manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate; or

4. Notarization by a notary, provided that the CA independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer.

3.2.2.2.9 Verification of Approval of EV Code Signing Certificate Request

1. **Verification Requirements**: In cases where an EV Code Signing Certificate Request is submitted by a Certificate Requester, before the CA issues the requested EV Code Signing Certificate, the CA MUST verify that an authorized Certificate Approver reviewed and approved the EV Code Signing Certificate Request.

2. **Acceptable Methods of Verification**: Acceptable methods of verifying the Certificate Approver's approval of an EV Code Signing Certificate Request include:

    1. Contacting the Certificate Approver using a Verified Method of Communication for the Applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV Code Signing Certificate Request;
    2. Notifying the Certificate Approver that one or more new EV Code Signing Certificate Requests are available for review and approval at a designated access-controlled and secure Web site, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the Web site; or
    3. Verifying the signature of the Certificate Approver on the EV Code Signing Certificate Request in accordance with Section 3.2.2.2.8.

3.2.2.2.10 Verification of Certain Information Sources

3.2.2.2.10.1 Verified Legal Opinion

1. **Verification Requirements**: Before relying on a legal opinion submitted to the CA, the CA MUST verify that such legal opinion meets the following requirements:

    1. **Status of Author**: The CA MUST verify that the legal opinion is authored by an independent legal practitioner retained by and representing the Applicant (or an in-house legal practitioner employed by the Applicant) (Legal Practitioner) who is either:

        1. A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility, or
        2. A Latin Notary who is currently commissioned or licensed to practice in the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary);

    2. **Basis of Opinion**: The CA MUST verify that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Legal Opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the Legal Practitioner's professional judgment and expertise;

    3. **Authenticity**: The CA MUST confirm the authenticity of the Verified Legal Opinion.

2. **Acceptable Methods of Verification**: Acceptable methods of establishing the foregoing requirements for a Verified Legal Opinion are:

    1. **Status of Author**: The CA MUST verify the professional status of the author of the legal opinion by directly contacting the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction;

    2. **Basis of Opinion**: The text of the legal opinion MUST make it clear that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the legal opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The legal opinion MAY also include disclaimers and other limitations customary in the Legal Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Legal Practitioner, should the legal opinion prove to be erroneous. An acceptable form of legal opinion is attached as Appendix B;

    3. **Authenticity**: To confirm the authenticity of the legal opinion, the CA MUST make a telephone call or send a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner, and obtain confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Legal Practitioner in records provided by the applicable phone company, QGIS, or QIIS.

        In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Section 3.2.2.2.10.1 (2)(i), no further verification of authenticity is required.

3.2.2.2.10.2 Verified Accountant Letter

1. **Verification Requirements**: Before relying on an accountant letter submitted to the CA, the CA MUST verify that such accountant letter meets the following requirements:

    1. **Status of Author**: The CA MUST verify that the accountant letter is authored by an Accounting Practitioner retained or employed by the Applicant and licensed within the country of the Applicant's Jurisdiction of Incorporation, Jurisdiction of Registration, or country where the Applicant maintains an office or physical facility. Verification of license MUST be through the member organization or regulatory organization in the Accounting Practitioner's country or jurisdiction that is appropriate to contact when verifying an accountant's license to practice in that country or jurisdiction. Such country or jurisdiction must have an accounting standards body that maintains full membership status with the International Federation of Accountants.
    2. **Basis of Opinion**: The CA MUST verify that the Accounting Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the Accounting Practitioner's professional judgment and expertise;
    3. **Authenticity**: The CA MUST confirm the authenticity of the Verified Accountant Letter.

2. **Acceptable Methods of Verification**: Acceptable methods of establishing the foregoing requirements for a Verified Accountant Letter are listed here.

1. **Status of Author**: The CA MUST verify the professional status of the author of the accountant letter by directly contacting the authority responsible for registering or licensing such Accounting Practitioners in the applicable jurisdiction.
2. **Basis of Opinion**: The text of the Verified Accountant Letter MUST make clear that the Accounting Practitioner is acting on behalf of the Applicant and that the information in the letter is based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The Verified Accountant Letter MAY also include disclaimers and other limitations customary in the Accounting Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Accounting Practitioner, should the Verified Accountant Letter prove to be erroneous. Acceptable forms of Verified Accountant Letter are attached as Appendix C.
3. **Authenticity**: To confirm the authenticity of the accountant's opinion, the CA MUST make a telephone call or send a copy of the Verified Accountant Letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioners and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Accountant in records provided by the applicable phone company, QGIS, or QIIS.

   In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Section 3.2.2.2.10.2 (2)(i), no further verification of authenticity is required.

3.2.2.2.10.3 Face-to-Face Validation

1. **Verification Requirements**: Before relying on face-to-face vetting documents submitted to the CA, the CA MUST verify that the Third-Party Validator meets the following requirements:
   1. **Qualification of Third-Party Validator**: The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual's residency;
   2. **Document Chain of Custody**: The CA MUST verify that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated;
   3. **Verification of Attestation**: If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the attestation and vetting documents.
2. **Acceptable Methods of Verification**: Acceptable methods of establishing the foregoing requirements for vetting documents are:
   1. **Qualification of Third-Party Validator**: The CA MUST verify the professional status of the Third-Party Validator by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction;
   2. **Document Chain of Custody**: The Third-Party Validator MUST submit a statement to the CA which attests that they obtained the Vetting Documents submitted to the CA for the individual during a face-to-face meeting with the individual;

3. **Verification of Attestation**: If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the vetting documents received from the Third-Party Validator. The CA MUST make a telephone call to the Third-Party Validator and obtain confirmation from them or their assistant that they performed the face-to-face validation. The CA MAY rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents, and the identity of the signer as verified by the CA in section 3.2.2.2.10.3 (1)(i), no further verification of authenticity is required.

3.2.2.2.10.4 Independent Confirmation From Applicant

An Independent Confirmation from the Applicant is a confirmation of a particular fact (e.g., confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV Authority of a Certificate Approver, etc.) that is:

1. Received by the CA from a Confirming Person (someone other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact, and who represents that he/she has confirmed such fact;
2. Received by the CA in a manner that authenticates and verifies the source of the confirmation; and
3. Binding on the Applicant.

An Independent Confirmation from the Applicant MAY be obtained via the following procedure:

1. **Confirmation Request**: The CA MUST initiate a Confirmation Request via an appropriate out-of-band communication, requesting verification or confirmation of the particular fact at issue as follows:
    1. **Addressee**: The Confirmation Request MUST be directed to:
        1. A position within the Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and is identified by name and title in a current QGIS, QIIS, QTIS, Verified Legal Opinion, Verified Accountant Letter, or by contacting the Applicant using a Verified Method of Communication; or
        2. The Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation as listed in the official records of the Incorporating Agency, with instructions that it be forwarded to an appropriate Confirming Person; or
        3. A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with these Guidelines).
    2. **Means of Communication**: The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:
        1. By paper mail addressed to the Confirming Person at:
            1. The address of the Applicant's Place of Business as verified by the CA in accordance with these Guidelines, or
            2. The business address for such Confirming Person specified in a current QGIS, QTIS, QIIS, Verified Professional Letter, or
            3. The address of the Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation, or

2. By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter; or
3. By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of the Applicant's Place of Business (verified in accordance with these Guidelines) and asking to speak to such person, and a person taking the call identifies him- or herself as such person; or
4. By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.

2. **Confirmation Response**: The CA MUST receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact at issue. Such response MAY be provided to the CA by telephone, by e-mail, or by paper mail, so long as the CA can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.
3. The CA MAY rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. The CA MAY rely on this verified contact information for future correspondence with the Confirming Person if:
    1. The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias;
    2. The Confirming Person's telephone/fax number is verified by the CA to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

3.2.2.2.10.5 Qualified Independent Information Source

A Qualified Independent Information Source (QIIS) is a regularly-updated and publicly available database that is generally recognized as a dependable source for certain information. A database qualifies as a QIIS if the CA determines that:

1. Industries other than the certificate industry rely on the database for accurate location, contact, or other information; and
2. The database provider updates its data on at least an annual basis.

The CA SHALL use a documented process to check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider's terms of use. The CA SHALL NOT use any data in a QIIS that the CA knows is

1. self-reported and
2. not verified by the QIIS as accurate.

Databases in which the CA or its owners or affiliated companies maintain a controlling interest, or in which any Registration Authorities or subcontractors to whom the CA has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest, do not qualify as a QIIS.

3.2.2.2.10.6 Qualified Government Information Source

A Qualified Government Information Source (QGIS) is a regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Government Entity, the reporting of data is required by law, and false or

misleading reporting is punishable with criminal or civil penalties. Nothing in these Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.

3.2.2.2.10.7 Qualified Government Tax Information Source

A Qualified Government Tax Information Source is a Qualified Government Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g., the IRS in the United States).

3.2.2.2.11 Parent/Subsidiary/Affiliate Relationship

A CA verifying an Applicant using information of the Applicant's Parent, Subsidiary, or Affiliate, when allowed under Section 3.2.2.2.3, Section 3.2.2.2.4, or Section 3.2.2.2.5, MUST verify the Applicant's relationship to the Parent, Subsidiary, or Affiliate. Acceptable methods of verifying the Applicant's relationship to the Parent, Subsidiary, or Affiliate include the following:

1. QIIS or QGIS: The relationship between the Applicant and the Parent, Subsidiary, or Affiliate is identified in a QIIS or QGIS;
2. Independent Confirmation from the Parent, Subsidiary, or Affiliate: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by obtaining an Independent Confirmation from the appropriate Parent, Subsidiary, or Affiliate (as described in Section 3.2.2.2.12);
3. Contract between CA and Parent, Subsidiary, or Affiliate: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a contract between the CA and the Parent, Subsidiary, or Affiliate that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;
4. Verified Professional Letter: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a Verified Professional Letter; or
5. Corporate Resolution: A CA MAY verify the relationship between an Applicant and a Subsidiary by relying on a properly authenticated corporate resolution that approves creation of the Subsidiary or the Applicant, provided that such resolution is:
    1. certified by the appropriate corporate officer (e.g., secretary), and
    2. the CA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.

3.2.2.2.12 Independent Confirmation From Applicant

An Independent Confirmation from the Applicant is a confirmation of a particular fact (e.g., confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV Authority of a Certificate Approver, etc.) that is:

1. Received by the CA from a Confirming Person (someone other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact, and who represents that he/she has confirmed such fact;
2. Received by the CA in a manner that authenticates and verifies the source of the confirmation; and
3. Binding on the Applicant.

An Independent Confirmation from the Applicant MAY be obtained via the following procedure:

1. **Confirmation Request**: The CA MUST initiate a Confirmation Request via an appropriate out-of-band communication, requesting verification or confirmation of the particular fact at issue as follows:
    1. **Addressee**: The Confirmation Request MUST be directed to:
        1. A position within the Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and is identified by name and title in a current QGIS, QIIS, QTIS, Verified Legal Opinion, Verified Accountant Letter, or by contacting the Applicant using a Verified Method of Communication; or
        2. The Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation as listed in the official records of the Incorporating Agency, with instructions that it be forwarded to an appropriate Confirming Person; or
        3. A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with these Guidelines).
    2. **Means of Communication**: The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:
        1. By paper mail addressed to the Confirming Person at:
            1. The address of the Applicant's Place of Business as verified by the CA in accordance with these Guidelines, or
            2. The business address for such Confirming Person specified in a current QGIS, QTIS, QIIS, Verified Professional Letter, or
            3. The address of the Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation, or
        2. By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter; or
        3. By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of the Applicant's Place of Business (verified in accordance with these Guidelines) and asking to speak to such person, and a person taking the call identifies him- or herself as such person; or
        4. By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.
2. **Confirmation Response**: The CA MUST receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact at issue. Such response MAY be provided to the CA by telephone, by e-mail, or by paper mail, so long as the CA can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.
3. The CA MAY rely on a verified Confirming Person to confirm their own contact information:

email address, telephone number, and facsimile number. The CA MAY rely on this verified contact information for future correspondence with the Confirming Person if:

1. The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias;
2. The Confirming Person's telephone/fax number is verified by the CA to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

3.2.3 Authentication of individual identity

Prior to issuing a Code Signing Certificate to an Individual Applicant, the CA MUST verify the Subject's Identity and authenticity of the Identity as follows.

3.2.3.1 Individual identity verification

The CA MUST verify the Applicant's identity using one of the following processes:

1. The CA MUST obtain a legible copy, which discernibly shows the Certificate Requester's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type). The CA MUST inspect the copy for any indication of alteration or falsification. The CA MUST also verify the address of the Certificate Requester using
    1. a government-issued photo ID,
    2. a QIIS or QGIS, or
    3. an access code to activate the Certificate where the access code was physically mailed to the Certificate Requester; OR
2. The CA MUST have the Certificate Requester digitally sign the Certificate Request using a valid personal Certificate that was issued under one of the following adopted standards: Qualified Certificates issued pursuant to ETSI TS 101 862, IGTF, Adobe Signing Certificate issued under the AATL or CDS program, the Kantara identity assurance framework at level 2, NIST SP 800-63 at level 2, or the FBCA CP at Basic or higher assurance.

3.2.3.2 Authenticity of Certificate requests for Individual Applicants

The CA MUST verify the authenticity of the Certificate Request using one of the following:

1. Having the Certificate Requester provide a photo of the Certificate Requester holding the submitted government-issued photo ID where the photo is of sufficient quality to read both the name listed on the photo ID and the issuing authority; OR
2. Having the CA perform an in-person or web camera-based verification of the Certificate Requester where an employee or contractor of the CA can see the Certificate Requester, review the Certificate Requester's photo ID, and confirm that the Certificate Requester is the individual identified in the submitted photo ID; OR
3. Having the CA obtain an executed Declaration of Identity of the Certificate Requester that includes at least one unique biometric identifier (such as a fingerprint or handwritten signature). The CA MUST confirm the document's authenticity directly with the Verifying Person using contact information confirmed with a QIIS or QGIS; OR
4. Verifying that the digital signature used to sign the Request under item (2) of Section 3.2.3.1 is a valid signature and originated from a Certificate issued at the appropriate level of assurance as evidenced by the certificate chain. Acceptable verification under this section includes validation that the Certificate was issued by a CA qualified by the entity responsible

for adopting, enforcing, or maintaining the adopted standard and chains to an intermediate certificate or root certificate designated as complying with such standard.

3.2.4 Non-verified subscriber information

3.2.5 Validation of authority

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

The CA MAY use the sources listed in Section 3.2.2.1.1 to verify the Reliable Method of Communication. Provided that the CA uses a Reliable Method of Communication, the CA MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

In addition, the CA SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA SHALL NOT accept any certificate requests that are outside this specification. The CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for interoperation

The CA SHOULD issue Code Signing and Timestamp Certificates that allow Application Software Suppliers to test their software with Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHOULD issue and make available to Application Software Suppliers upon request Code Signing and Timestamp Certificates that are valid (non-revoked and unexpired).

3.2.7 Data source accuracy

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

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

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

3.2.8. Denied Lists and Other Legal Block Lists

This section is applicable for EV Code Signing Certificate Requests.

1. **Verification Requirements**: The CA MUST verify whether the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Business:

1. Is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or
2. Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business.

The CA MUST NOT issue any EV Code Signing Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Registration or Place of Business is on any such list.

2. **Acceptable Methods of Verification**: The CA MUST take reasonable steps to verify with the following lists and regulations:

    1. If the CA has operations in the U.S., the CA MUST take reasonable steps to verify with the following US Government denied lists and regulations:

        1. BIS Denied Persons List - https://www.bis.doc.gov/index.php/the-denied-persons-list
        2. BIS Denied Entities List - https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list
        3. US Treasury Department List of Specially Designated Nationals and Blocked Persons - https://www.treasury.gov/resource-center/sanctions/sdn-list/pages/default.aspx
        4. US Government export regulations

    2. If the CA has operations in any other country, the CA MUST take reasonable steps to verify with all equivalent denied lists and export regulations (if any) in such other country.

3.2.9 Final Cross-Correlation and Due Diligence

1. The results of the verification processes and procedures outlined in these Guidelines are intended to be viewed both individually and as a group. Thus, after all of the verification processes and procedures are completed, the CA MUST have a person who is not responsible for the collection of information review all of the information and documentation assembled in support of the EV Code Signing Certificate application and look for discrepancies or other details requiring further explanation.
2. The CA MUST obtain and document further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve those discrepancies or details that require further explanation.
3. The CA MUST refrain from issuing an EV Code Signing Certificate until the entire corpus of information and documentation assembled in support of the EV Code Signing Certificate Request is such that issuance of the EV Code Signing Certificate will not communicate factual information that the CA knows, or the exercise of due diligence should discover from the assembled information and documentation, to be inaccurate,. If satisfactory explanation and/or additional documentation are not received within a reasonable time, the CA MUST decline the EV Code Signing Certificate Request and SHOULD notify the Applicant accordingly.
4. In the case where some or all of the documentation used to support the application is in a language other than the CA's normal operating language, the CA or its Affiliate MUST

perform the requirements of this Final Cross-Correlation and Due Diligence section using employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in Section 5.3. When employees under the control of the CA do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA MAY:

1. Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or
2. When the CA has utilized the services of an RA, the CA MAY rely on the language skills of the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with Section 3.2.9, Subsections (1), (2) and (3). Notwithstanding the foregoing, prior to issuing the EV Code Signing Certificate, the CA MUST review the work completed by the RA and determine that all requirements have been met; or
3. When the CA has utilized the services of an RA, the CA MAY rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with this section and is subjected to the Audit Requirements of Section 8.7 and Section 8.2.

In the case of EV Code Signing Certificates to be issued in compliance with the requirements of Section 1.3.2.1, the Enterprise RA MAY perform the requirements of this Final Cross-Correlation and Due Diligence section.

3.2.10 Disclosure of Verification Sources

Effective as of 15 March 2025, prior to the use of an Incorporating Agency or Registration Agency to fulfill these verification requirements, the CA MUST publicly disclose Agency Information about the Incorporating Agency or Registration Agency. This disclosure SHALL be through an appropriate and readily accessible online means.

This Agency Information SHALL include at least the following:

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

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

3.3.2 Identification and authentication for re-key after revocation

3.4 Identification and authentication for revocation request

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

For EV Code Signing Certificates, the CA MAY only issue to Applicants that meet the Private Organization, Government Entity, Business Entity and Non-Commercial Entity requirements specified below.

The CA SHALL implement procedures to identify suspicious certificate requests as defined in Section 3.2.2.8.

4.1.1.1 Private Organization Subjects

An Applicant qualifies as a Private Organization if:

1. The entity's legal existence is created or recognized by a by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation, registration number, etc.) or created or recognized by a Government Agency (e.g. under a charter, treaty, convention, or equivalent recognition instrument);
2. The entity designated with the Incorporating or Registration Agency a Registered Agent, a Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration), or an equivalent facility;
3. The entity is not designated on the records of the Incorporating or Registration Agency by labels such as "inactive," "invalid," "not current," or the equivalent;
4. The entity has a verifiable physical existence and business presence;
5. The entity's Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
6. The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

4.1.1.2 Government Entity Subjects

An Applicant qualifies as a Government Entity if:

1. The entity's legal existence was established by the political subdivision in which the entity operates;
2. The entity is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
3. The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

4.1.1.3 Business Entity Subjects

An Applicant qualifies as a Business Entity if:

1. The entity is a legally recognized entity that filed certain forms with a Registration Agency in its jurisdiction, the Registration Agency issued or approved the entity's charter, certificate, or license, and the entity's existence can be verified with that Registration Agency;

2. The entity has a verifiable physical existence and business presence;
3. At least one Principal Individual associated with the entity is identified and validated by the CA;
4. The identified Principal Individual attests to the representations made in the Subscriber Agreement;
5. The CA verifies the entity's use of any assumed name used to represent the entity pursuant to the requirements of Section 3.2.2.2.2;
6. The entity and the identified Principal Individual associated with the entity are not located or residing in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
7. The entity and the identified Principal Individual associated with the entity are not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

4.1.1.4 Non-Commercial Entity Subjects

An Applicant qualifies as a Non-Commercial Entity if:

1. The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. The CA/Browser Forum may publish a listing of Applicants who qualify as an International Organization for EV eligibility; and
2. The Applicant is not headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
3. The Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

Subsidiary organizations or agencies of an entity that qualifies as a Non-Commercial Entity also qualifies for EV Code Signing Certificates as a Non-Commercial Entity.

4.1.2 Enrollment process and responsibilities

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

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The certificate request MAY include all factual information about the Applicant necessary to issue the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA MUST obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm

it with the Applicant. The CA MUST establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Prior to issuing a Code Signing Certificate, each CA SHOULD check at least one database containing information about known or suspected producers, publishers, or distributors of Suspect Code, as identified or indicated by an Anti-Malware Organization and any database of deceptive names maintained by an Application Software Provider. The CA MUST also maintain and check an internal database listing Certificates revoked due to Code Signatures on Suspect Code and previous certificate requests rejected by the CA. The CA MUST use this internal database to follow the additional procedures defined in Section 4.2.2 of this document to ensure that the Applicant will protect its Private Keys and not sign Suspect Code.

Prior to issuing Code Signing Certificates, the CA SHALL perform "due diligence" verification as specified in Section 3.2.9.

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

For Non-EV Code Signing Certificates, the CA MAY use the documents and data provided in Section 3.2 to verify certificate information, or may reuse previous validations themselves, provided that the CA obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 825 days prior to issuing the Certificate.

For EV Code Signing Certificates, use of documents, data, and previous validations performed per Section 3.2 SHALL be governed by the usage periods as defined in Section 4.2.1.1.

4.2.1.1 Requirements for Re-use of Existing Documentation for EV Code Signing Certificates

For each EV Code Signing Certificate Request, including requests to renew existing EV Code Signing Certificates, the CA MUST perform all authentication and verification tasks required to ensure that the request is properly authorized by the Applicant and that the information in the EV Code Signing Certificate is still accurate and valid. This section sets forth the age limitations for the use of documentation collected by the CA for EV Code Signing Certificates.

4.2.1.1.1 Validation For Existing EV Subscribers

If an Applicant has a currently valid EV Code Signing Certificate issued by the CA, a CA MAY rely on its prior authentication and verification of:

1. The Principal Individual verified under Section 3.2.2.2.1.2 (4) if the individual is the same person as verified by the CA in connection with the Applicant's previously issued and currently valid EV Code Signing Certificate;
2. The Applicant's Place of Business under Section 3.2.2.2.3.1;
3. The Applicant's Verified Method of Communication required by Section 3.2.2.2.4 but still MUST perform the verification required by subsection (2) (ii);
4. The Applicant's Operational Existence under Section 3.2.2.2.5; and
5. The Name, Title, Agency and Authority of the Contract Signer, and Certificate Approver, under Section 3.2.2.2.7.

4.2.1.1.2 Re-issuance Requests

A CA may rely on a previously verified EV Code Signing Certificate request to issue a replacement certificate, so long as the certificate being referenced was not revoked due to fraud or other illegal

conduct, if:

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

4.2.1.1.3 Age of Validated Data

1. Except for reissuance of an EV Code Signing Certificate under Section 4.2.1.1.2 and except when permitted otherwise in Section 4.2.1.1.1, the age of all data used to support issuance of an EV Code Signing Certificate (before revalidation is required) SHALL NOT exceed the following limits:
    1. Legal existence and identity – 398 days;
    2. Assumed name – 398 days;
    3. Address of Place of Business – 398 days;
    4. Verified Method of Communication – 398 days;
    5. Operational existence – 398 days;
    6. Name, Title, Agency, and Authority – 398 days, unless a contract between the CA and the Applicant specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of EV roles until revoked by the Applicant or CA, or until the contract expires or is terminated.
2. The 398-day period set forth above SHALL begin to run on the date the information was collected by the CA.
3. The CA MAY reuse a previously submitted EV Code Signing Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single EV Code Signing Certificate Request in support of multiple EV Code Signing Certificates containing the same Subject to the extent permitted under Section 3.2.2.2.8 and Section 3.2.2.2.9.
4. The CA MUST repeat the verification process required in these Guidelines for any information obtained outside the time limits specified above except when permitted otherwise under Section 4.2.1.1.1.

4.2.2 Approval or rejection of certificate applications

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

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

Except where issuance is expressly authorized by the Application Software Supplier, CAs MUST not issue new Code Signing Certificates to an entity where the CA is aware that the entity has been the victim of two Takeover Attacks or where the CA is aware that entity breached a requirement under this Section to protect Private Keys under Section 6.2.7.4.1(1) or Section 6.2.7.4.1(2).

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

4.3.2 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

Prior to 2024-04-15, the CA SHALL treat revocation of Certificates in accordance with the requirements specified in Section 4.9 of these Requirements or Section 4.9 specified in version 3.2.0 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates. Effective 2024-04-15, the CA SHALL treat revocation of Certificates in accordance with Section 4.9 specified in these Requirements.

4.9.1 Circumstances for revocation

When revocation of a Subscriber Certificate is done due to a Key Compromise or use in Suspect Code the CA SHALL determine an appropriate value for the revocationDate based on its own investigation. The CA SHALL set a historic date as revocationDate if deemed appropriate.

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;
5. 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; or
6. The CA has reasonable assurance that a Certificate was used to sign Suspect Code.

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:

7. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
8. The CA obtains evidence that the Certificate was misused.
9. 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.
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 Certificate Policy or Certification Practice Statement.
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 Certificate Policy and/or Certification Practice Statement.

The CA MAY delay revocation based on a request from Application Software Suppliers where immediate revocation has a potentially large negative impact to the ecosystem.

Note: Nothing herein prohibits a CA from revoking a Code Signing Certificate prior to these time frames.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.

4.9.2 Who can request revocation

The CA MUST provide Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions on how they can report suspected Private Key compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA MUST publicly disclose the instructions on its website.

4.9.3 Procedure for revocation request

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

The CA SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other

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

4.9.4 Revocation request grace period

4.9.5 Time within which CA must process the revocation request

The CA MUST maintain a continuous 24x7 ability to communicate with Anti-Malware Organizations, Application Software Suppliers, and law enforcement agencies and respond to high-priority Certificate Problem Reports, such as reports requesting revocation of Certificates used to sign malicious code, fraud, or other illegal conduct.

The CA MUST acknowledge receipt of plausible notices about Suspect Code signed with a certificate issued by the CA or a Subordinate CA.

The CA MUST begin investigating Certificate Problem Reports within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the alleged problem (adware, spyware, malware, software bug, etc.),
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber,
3. The entity making the report (for example, a notification from an Anti-Malware Organization or law enforcement agency carries more weight than an anonymous complaint), and
4. Relevant legislation.

When revoking a Certificate, the CA SHOULD work with the Subscriber to estimate a date of when the revocation should occur in order to mitigate the impact of revocation on validly signed Code. For key compromise events, this date SHOULD be the earliest date of suspected compromise.

4.9.6 Revocation checking requirement for relying parties

A Certificate MAY have a one-to-one relationship or one-to-many relationship with the signed Code. Regardless, revocation of a Certificate may invalidate the Code Signatures on all signed Code, some of which could be perfectly sound. Because of this, the CA MAY specify the time at which the Certificate is first considered to be invalid in the `revocationDate` field of a CRL entry or the `revocationTime` field of an OCSP response to time-bind the set of software affected by the revocation[1], and software should continue to treat objects containing a timestamp dated before the revocation date as valid.

4.9.7 CRL issuance frequency

For the status of Subordinate CA Certificates:

- The Issuing CA SHALL publish a CRL, then update and reissue a CRL at least once every twelve months and within 24 hours after revoking a Subordinate CA Certificate. The `nextUpdate` field MUST NOT be more than twelve months beyond the value of the `thisUpdate` field.

[1]Backdating the `revocationDate` field is an exception to best practice described in RFC 5280 (section 5.3.2); however, these Requirements specify the use of the `revocationDate` field to convey the “invalidity date” to support Application Software Supplier software implementations that process the `revocationDate` field as the date when the Certificate is first considered to be invalid.

For the status of Code Signing Certificates:

- The Subordinate CA SHALL publish a CRL, then update and reissue a CRL at least once every seven days, and the value of the `nextUpdate` field MUST NOT be more than ten days beyond the value of the `thisUpdate` field.

For the status of Timestamp Certificates:

- The Subordinate CA SHALL update and reissue CRLs at least once every twelve months and within 24 hours after revoking a Timestamp Certificate, and the value of the `nextUpdate` field MUST 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

OCSP responses MUST conform to RFC6960 and/or RFC5019. OCSP responses MUST either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type `id-pkix-ocsp-nocheck`, as defined by RFC6960.

4.9.10 On-line revocation checking requirements

Effective 2023-09-15, OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

Effective 2023-09-15, 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.

CAs MAY provide OCSP responses for Code Signing Certificates and Timestamp Certificates for the time period specified in their CPS, which MAY be at least 10 years after the expiration of the certificate.

If the CA provides OCSP responses, the CA SHALL support an OCSP capability using the GET method for Certificates issued in accordance with these Requirements.

For the status of Subordinate CA Certificates:

- If the Issuing CA provides OCSP responses, the Issuing CA SHALL update information provided via an OCSP response at least every twelve months and within 24 hours after revoking a Subordinate CA Certificate.

For the status of Code Signing Certificates:

- If the Subordinate CA provides OCSP responses, the CA SHALL update information provided via an OCSP response at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.

For the status of Timestamp Certificates:

- If the Subordinate CA provides OCSP responses, the Subordinate CA SHALL update information provided via an OCSP response at least every twelve months and within 24 hours after revoking a Timestamp Certificate.

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.

If the OCSP responder receives a request for the status of a certificate serial number that is not “assigned”, then the responder MUST NOT respond with a “good” status.

4.9.11 Other forms of revocation advertisements available

Because some Application Software Suppliers utilize non-standard revocation mechanisms, CAs MUST, if requested by the Application Software Supplier and using a method of communication specified by the Application Software Vendor, notify the Application Software Supplier whenever the CA revokes a Code Signing Certificate because (i) the CA mis-issued the Certificate, (ii) the Certificate was used to sign Suspect Code, or (iii) there is a suspected or actual compromise of the Applicant’s or CA’s Private Key.

4.9.12 Special requirements re key compromise

See Section 4.9.1.

4.9.13 Circumstances for suspension

Effective 2023-09-15, the Repository MUST NOT include entries that indicate that a Certificate is suspended.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

Revocation entries on an OCSP response MUST remain for the same amount of time as for the CRL entries, as described in Section 7.2.

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.

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

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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

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

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

The Certificate Management Process MUST include:

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

The CA's security program MUST include an annual risk assessment that:

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

Based on the risk assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST also take into account then-available technology and the cost of implementing the specific measures, and SHALL implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical controls

5.1.1 Site location and construction

5.1.2 Physical access

5.1.3 Power and air conditioning

5.1.4 Water exposures

5.1.5 Fire prevention and protection

5.1.6 Media storage

5.1.7 Waste disposal

5.1.8 Off-site backup

5.2 Procedural controls

5.2.1 Trusted roles

5.2.2 Number of 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

5.2.4 Roles requiring separation of duties

1. The CA MUST enforce rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Code Signing Certificate. The Final Cross-Correlation and Due Diligence steps, as outlined in Section 3.2.9, MAY be performed by one of the persons. For example, one Validation Specialist MAY review and verify all the Applicant information and a second Validation Specialist MAY approve issuance of the EV Code Signing Certificate.
2. Such controls MUST be auditable.

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

Prior to the commencement of employment of any person by the CA for engagement in the EV Processes, whether as an employee, agent, or an independent contractor of the CA, the CA MUST:

1. **Verify the identity of such person**: Verification of identity MUST be performed through:
    1. The personal (physical) presence of such person before trusted persons who perform human resource or security functions, and
    2. The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or drivers licenses);

and

2. **Verify the trustworthiness of such person**: Verification of trustworthiness SHALL include background checks, which address at least the following, or their equivalent:
    1. Confirmation of previous employment,
    2. Check of professional references;
    3. Confirmation of the highest or most-relevant educational qualification obtained;
    4. Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction in which the person will be employed;

    and

3. In the case of employees already in the employ of the CA at the time of adoption of these Guidelines whose identity and background has not previously been verified as set forth above, the CA SHALL conduct such verification within three months of the date of adoption of these Guidelines.

5.3.3 Training requirements and procedures

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

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

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

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

If a Validation Specialist is to be engaged in the EV Processes, the required internal examination must relate to the EV Code Signing Certificate validation criteria outlined in these Guidelines.

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

5.3.6 Sanctions for unauthorized actions

5.3.7 Independent contractor 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

5.4 Audit logging procedures

5.4.1 Types of events recorded

5.4.1.1 Types of events recorded for CAs

The CA and each Delegated Third Party SHALL record details of the 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 management events, including:

1. Key generation, backup, storage, recovery, archival, and destruction;
2. Certificate requests, renewal, and re-key requests, and revocation;
3. Approval and rejection of certificate requests ;
4. Cryptographic device lifecycle management events;
5. Generation of Certificate Revocation Lists
6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10); and
7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles
8. CA and Subscriber lifecycle management events, including:
    1. Certificate requests, renewals, re-key requests, and revocation;
    2. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement (CPS);
    3. Acceptance and rejection of certificate requests;
    4. Issuance of Certificates;
    5. Generation of Certificate Revocation Lists and OCSP entries; and
    6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).
9. Security events, including:
    1. Successful and unsuccessful PKI system access attempts;
    2. PKI and security system actions performed;
    3. Security profile changes;
    4. System crashes, hardware failures, and other anomalies;
    5. Firewall and router activities; and
    6. Entries to and exits from the CA facility.

Log records MUST include the following elements:

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

5.4.1.2 Types of events recorded for Timestamp Authorities

The Timestamp Authority MUST log the following information and make these records available to its Qualified Auditor as proof of the Timestamp Authority's compliance with these Requirements:

1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
2. History of the timestamp server configuration,
3. Any attempt to delete or modify timestamp logs,
4. Security events, including:
    1. Successful and unsuccessful Timestamp Authority access attempts;
    2. Timestamp Authority server actions performed;
    3. Security profile changes;
    4. System crashes and other anomalies; and
    5. Firewall and router activities;
5. Revocation of a timestamp certificate,
6. Major changes to the timestamp server's time, and
7. System startup and shutdown.

5.4.2 Frequency of processing log

5.4.3 Retention period for audit log

The CA, Delegated Third Parties, and Timestamp Authority MUST 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)(1) after the later occurrence of:
    1. the destruction of the CA Private Key; or
    2. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1.2)(2) after the revocation or expiration of the Subscriber Certificate;
3. Timestamp Authority data records (as set forth in Section 5.4.1.2) after the revocation or renewal of the Timestamp Certificate Private Key (as set forth in Section 6.3.2);
4. Any security event records (as set forth in Section 5.4.1.1(3) and for Timestamp Authority security event records set forth in Section 5.4.1.2(3)) after the event occurred

Note: While these Requirements set the minimum retention period, the CA, Delegated Third Parties, and Timestamp Authority 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 events.

5.4.4 Protection of audit log

5.4.5 Audit log backup procedures

5.4.6 Audit collection system (internal vs. external)

5.4.7 Notification to event-causing subject

5.4.8 Vulnerability assessments

Additionally, the CA's security program MUST include an annual risk assessment that:

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

5.5 Records archival

5.5.1 Types of records archived

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

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

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

5.5.2 Retention period for archive

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

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

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

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

5.5.3 Protection of archive

5.5.4 Archive backup procedures

5.5.5 Requirements for time-stamping of records

5.5.6 Archive collection system (internal or external)

5.5.7 Procedures to obtain and verify archive information

5.6 Key changeover

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

CA organizations shall have an incident response plan and a disaster recovery plan.

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

The business continuity plan MUST include:

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

5.7.2 Computing resources, software, and/or data are corrupted

5.7.3 Entity private key compromise procedures

5.7.4 Business continuity capabilities after a disaster

5.8 CA or RA termination

If the CA wishes to stop supporting validation of Code Signing Certificates or Timestamp Certificates prior to the date specified in its Certificate Policy/Certificate Practice Statement, the CA MUST give 90 days' prior notice to all Application Software Suppliers relying on the root

certificate and permit the Application Software Suppliers sufficient time to take appropriate action as determined by the Application Software Supplier.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA Key Pair Generation

For CA Key Pairs that are either

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

the CA SHALL:

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

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

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

In all cases, the CA SHALL:

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

6.1.1.2 RA Key Pair Generation

6.1.1.3 Subscriber Key Pair Generation

The CA SHALL reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;

4. The CA has previously been 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).

6.1.2 Private key delivery to subscriber

If the CA or any Delegated Third Party is generating the Private Key on behalf of the Subscriber where the Private Keys will be transported to the Subscriber outside of the Signing Service's secure infrastructure, then the entity generating the Private Key MUST transport the Private Key in hardware with an activation method that is equivalent to 128 bits of encryption.

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

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

6.1.3 Public key delivery to certificate issuer

6.1.4 CA public key delivery to relying parties

6.1.5 Key sizes

6.1.5.1 Root and Subordinate CA key sizes

For Keys corresponding to Root and Subordinate CAs:

- If the Key is RSA, then the modulus MUST be at least 4096 bits in length. [2]
- If the Key is ECDSA, then the curve MUST be one of NIST P-256, P-384, or P-521.
- If the Key is DSA, then one of the following key parameter options MUST be used:
  - Key length (L) of 2048 bits and modulus length (N) of 224 bits
  - Key length (L) of 2048 bits and modulus length (N) of 256 bits

6.1.5.2 Code signing Certificate and Timestamp Authority key sizes

For Keys corresponding to Subscriber code signing and Timestamp Authority Certificates:

- If the Key is RSA, then the modulus MUST be at least 3072 bits in length.
- If the Key is ECDSA, then the curve MUST be one of NIST P-256, P-384, or P-521.
- If the Key is DSA, then one of the following key parameter options MUST be used:
  - Key length (L) of 2048 bits and modulus length (N) of 224 bits
  - Key length (L) of 2048 bits and modulus length (N) of 256 bits

6.1.6 Public key parameters generation and quality checking

RSA: The CA SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^16 + 1 and 2^256 - 1.

[2] CAs MAY sign Cross-Certificates with Root CA RSA Private Keys whose modulus length is less than 4096 bits, provided that the Cross-Certificate is issued to a Root CA whose Public Key adheres to the key size requirements of this section.

The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

ECDSA: The CA SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

6.1.7 Key usage purposes

Private Keys corresponding to Root Certificates MUST NOT be used to sign Certificates or create other Signatures 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);
4. Certificates for OCSP Response verification; and
5. Signatures for OCSP Responses.

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

6.2.1 Cryptographic module standards and controls

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

6.2.3 Private key escrow

6.2.4 Private key backup

See Section 5.2.2.

6.2.5 Private key archival

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

6.2.6 Private key transfer into or from a cryptographic module

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

The CA or Signing Service SHALL NOT transfer Private Keys from a cryptographic module to a Subscriber.

6.2.7 Private key storage on cryptographic module

6.2.7.1 Private key storage for CA keys

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.

6.2.7.2 Private key storage for Timestamp Authorities

A Timestamp Authority MUST protect its Private Key using a process that is at least to FIPS 140-2 level 3, Common Criteria EAL 4+ (ALC_FLR.2), or higher.

6.2.7.3 Private key storage for Signing Services

The Signing Service MUST ensure that a Subscriber's Private Key is generated, stored, and used in a secure environment that has controls to prevent theft or misuse. A Signing Service MUST enforce multi-factor authentication or server-to-server authentication to access and authorize Code Signing.

For Code Signing Certificates, Signing Services SHALL protect Subscriber Private Keys in a Hardware Crypto Module conforming to at least FIPS 140-2 level 3 or Common Criteria EAL 4+.

Techniques that MUST be used to satisfy this requirement include:

1. Use of an Hardware Crypto Module, verified by means of a FIPS or Common Criteria certificate; or
2. A cloud-based key generation and protection solution with the following requirements:
    1. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements;
    2. Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.

6.2.7.4 Subscriber Private Key protection and verification

6.2.7.4.1 Subscriber Private Key protection

For Non-EV Code Signing Certificates issued prior to June 1, 2023, the CA MUST obtain a representation from the Subscriber that the Subscriber will use one of the following options to generate and protect their Code Signing Certificate Private Keys:

1. A Trusted Platform Module (TPM) that generates and secures a Key Pair and that can document the Subscriber's Private Key protection through a TPM key attestation.
2. A suitable Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2, Common Criteria EAL 4+, or equivalent.
3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140-2 Level 2 or Common Criteria EAL 4+). The Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

For Non-EV Code Signing Certificates issued prior to June 1, 2023, a CA MUST recommend that the

Subscriber protect Private Keys using the method described in Section 6.2.7.4.1(1) or 6.2.7.4.1(2) over the method described in Section 6.2.7.4.1(3) and obligate the Subscriber to protect Private Keys in accordance with Section 9.6.3 (2).

For EV Code Signing Certificates issued prior to June 1, 2023, CAs SHALL ensure that the Subscriber's Private Key is generated, stored and used in a Hardware Crypto Module that meets or exceeds the requirements of FIPS 140-2 level 2 or Common Criteria EAL 4+. Acceptable methods of satisfying this requirement include (but are not limited to) the following:

4. The CA ships a suitable Hardware Crypto Module, with a preinstalled Private Key, in the form of a smartcard or USB device or similar;
5. The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate indicating that the Private Key is managed in a suitable Hardware Crypto Module;
6. The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 2.

Effective June 1, 2023, Subscriber Private Keys for Code Signing Certificates SHALL be protected per the following requirements. The CA MUST obtain a contractual representation from the Subscriber that the Subscriber will use one of the following options to generate and protect their Code Signing Certificate Private Keys in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+:

7. Subscriber uses a Hardware Crypto Module meeting the specified requirement;
8. Subscriber uses a cloud-base key generation and protection solution with the following requirements:
    1. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements;
    2. Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.
9. Subscriber uses a Signing Service which meets the requirements of Section 6.2.7.3.

6.2.7.4.2 Subscriber Private Key verification

CAs SHALL ensure that the Subscriber's Private Key is generated, stored, and used in a suitable Hardware Crypto Module that meets or exceeds the requirements specified in Section 6.2.7.4.1. One of the following methods MUST be employed to satisfy this requirement:

1. The CA ships a suitable Hardware Crypto Module, with one or more pre-generated Key Pairs that the CA has generated using the Hardware Crypto Module;
2. The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate, commonly known as key attestation, indicating that the Private Key was generated in a non-exportable way using a suitable Hardware Crypto Module;
3. The Subscriber uses a CA prescribed crypto library and a suitable Hardware Crypto Module combination for the Key Pair generation and storage;
4. The Subscriber provides an internal or external IT audit indicating that it is only using a suitable Hardware Crypto Module to generate Key Pairs to be associated with Code Signing Certificates;
5. The Subscriber provides a suitable report from the cloud-based key protection solution subscription and resources configuration protecting the Private Key in a suitable Hardware

Crypto Module;

6. The CA relies on a report provided by the Applicant that is signed by an auditor who is approved by the CA and who has IT and security training or is a CISA witnesses the Key Pair creation in a suitable Hardware Crypto Module solution including a cloud-based key generation and protection solution;
7. The Subscriber provides an agreement that they use a Signing Service meeting the requirements of Section 6.2.7.3;

6.2.8 Method of activating private key

6.2.9 Method of deactivating private key

6.2.10 Method of destroying private key

6.2.11 Cryptographic Module Rating

6.3 Other aspects of key pair management

6.3.1 Public key archival

6.3.2 Certificate operational periods and key pair usage periods

The validity period for a Code Signing Certificate issued to a Subscriber MUST NOT exceed 39 months.

The Timestamp Authority MUST use a new Timestamp Certificate with a new Private Key no later than every 15 months to minimize the impact to users in the event that a Timestamp Certificate's Private Key is compromised. The validity for a Timestamp Certificate must not exceed 135 months. The Timestamp Certificate MUST meet the requirements in Section 6.1.5 for the communicated time period.

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.2 Activation data protection

6.4.3 Other aspects of activation data

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

6.5.2 Computer security rating

6.6 Life cycle technical controls

6.6.1 System development controls

6.6.2 Security management controls

6.6.3 Life cycle security controls

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 for the CA, Signing Service and Timestamp Authority.

6.8 Time-stamping

If the CA issues Code Signing Certificates, then the CA MUST operate a Timestamp Authority that complies with RFC 3161. CAs MUST recommend to Subscribers that they use the CA's Timestamp Authority to timestamp signed code.

The Timestamp Authority MUST ensure that clock synchronization is maintained when a leap second occurs. A Timestamp Authority MUST synchronize its timestamp server at least every 24 hours with a UTC(k) time source. The timestamp server MUST automatically detect and report on clock drifts or jumps out of synchronization with UTC. Clock adjustments of one second or greater MUST be auditable events. Any changes to its signing process MUST be an auditable event.

The digest algorithm used to sign Timestamp tokens must match the digest algorithm used to sign the Timestamp Certificate.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

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

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

7.1.1 Version number(s)

Certificates MUST be of type X.509 v3.

7.1.2 Certificate extensions

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

7.1.2.1 Root CA Certificate

a. `basicConstraints`

   This extension MUST appear as a critical extension. The `cA` field MUST be set true. The `pathLenConstraint` field SHOULD NOT be present.

b. `keyUsage`

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

c. `certificatePolicies`

   This extension SHOULD NOT be present.

d. `extKeyUsage`

   This extension MUST NOT be present.

7.1.2.2 Subordinate CA Certificate

a. `certificatePolicies`

   This extension MUST be present and SHOULD NOT be marked critical.

   `certificatePolicies:policyIdentifier` Required; see Section 7.1.6.3 for requirements on Policy Identifiers.

   The following fields MUST be present if the Subordinate CA is not an Affiliate of the entity that controls the Root CA.

   - `certificatePolicies:policyQualifiers:policyQualifierId` (Optional)

     `id-qt 1` [RFC5280].

   - `certificatePolicies:policyQualifiers:qualifier:cPSuri` (Optional)

HTTP URL for the Root CA's Certificate Policies, Certification Practice Statement, Relying Party agreement, or other pointer to online policy information provided by the CA.

b. `cRLDistributionPoints`

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

c. `authorityInformationAccess`

   This extension MUST be present. It MUST NOT be marked critical.

   It MUST contain the HTTP URL of the Issuing CA's certificate (`accessMethod` = 1.3.6.1.5.5.7.48.2). If the CA provides OCSP responses, it MUST contain the HTTP URL of the Issuing CA's OCSP responder (`accessMethod` = 1.3.6.1.5.5.7.48.1).

d. `basicConstraints`

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

e. `keyUsage`

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

f. `extKeyUsage`

This extension MUST be present and SHOULD NOT be marked critical.

If the Subordinate CA will be used to issue Code Signing Certificates:

- `id-kp-codeSigning` MUST be present.
- `id-kp-timeStamping` MUST NOT be present.

If the Subordinate CA will be used to issue Timestamp Certificates:

- `id-kp-timeStamping` MUST be present.
- `id-kp-codeSigning` MUST NOT be present.

Additionally, the following EKUs MUST NOT be present:

- `anyExtendedKeyUsage`
- `id-kp-serverAuth`
- `id-kp-emailProtection`

Other values SHOULD NOT be present. If any other value is present, the CA MUST have a business agreement with a Platform vendor requiring that EKU in order to issue a Platform-specific code signing certificate with that EKU.

h. `authorityKeyIdentifier`

   This extension MUST be present and MUST NOT be marked critical.

7.1.2.3 Code signing and Timestamp Certificate

a. `certificatePolicies`

This extension MUST be present and SHOULD NOT be marked critical.

- `certificatePolicies:policyIdentifier` (Required)

  A Policy Identifier, defined by the issuing CA, that indicates a Certificate Policy asserting the issuing CA's adherence to and compliance with these Requirements.

The following fields MAY be present:

- `certificatePolicies:policyQualifiers:policyQualifierId` (Recommended)

  `id-qt 1` [RFC 5280].

- `certificatePolicies:policyQualifiers:qualifier:cPSuri` (Optional)

  HTTP URL for the Subordinate CA's Certification Practice Statement, Relying Party agreement or other pointer to online information provided by the CA.

b. `cRLDistributionPoints`

This extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service.

c. `authorityInformationAccess`

This extension MUST be present. It MUST NOT be marked critical.

It MUST contain the HTTP URL of the Issuing CA's certificate (`accessMethod` = 1.3.6.1.5.5.7.48.2). If the CA provides OCSP responses, it MUST contain the HTTP URL of the Issuing CA's OCSP responder (`accessMethod` = 1.3.6.1.5.5.7.48.1).

d. `basicConstraints` (optional)

The `cA` field MUST NOT be true.

e. `keyUsage`

This extension MUST be present and MUST be marked critical.

The bit position for `digitalSignature` MUST be set. Bit positions for `keyCertSign` and `cRLSign` MUST NOT be set. All other bit positions SHOULD NOT be set.

f. `extKeyUsage`

If the Certificate is a Code Signing Certificate, then `id-kp-codeSigning` MUST be present and the following EKUs MAY be present:

- Lifetime Signing OID (`1.3.6.1.4.1.311.10.3.13`)
- `id-kp-emailProtection`
- Document Signing (`1.3.6.1.4.1.311.3.10.3.12`)

If the Certificate is a Timestamp Certificate, then `id-kp-timeStamping` MUST be present and MUST be marked critical.

Additionally, the following EKUs MUST NOT be present:

- `anyExtendedKeyUsage`
- `id-kp-serverAuth`

Other values SHOULD NOT be present. If any other value is present, the CA MUST have a business agreement with a Platform vendor requiring that EKU in order to issue a Platform-specific code signing certificate with that EKU.

g. `authorityKeyIdentifier`

This extension MUST be present and MUST NOT be marked critical.

7.1.2.4 All Certificates

All other fields and extensions MUST 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.

CAs SHALL NOT issue a Certificate with:

a. 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
b. semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including an `extKeyUsage` value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.3 Algorithm object identifiers

7.1.3.1 SubjectPublicKeyInfo

As defined in Section 6.1.5.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a CA Private Key MUST conform to these requirements on the use of the `AlgorithmIdentifier` or `AlgorithmIdentifier`-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The `signatureAlgorithm` field of a Certificate.
- The `signature` field of a TBSCertificate.
- The `signatureAlgorithm` field of a CertificateList
- The `signature` field of a TBSCertList
- The `signatureAlgorithm` field of a BasicOCSPResponse
- The `digestAlgorithms` field of a SignedData corresponding to a Timestamp token

7.1.3.2.1 RSA

The CA SHALL use one of the following signature algorithms:

- RSASSA-PKCS1-v1_5 with SHA-256

- RSASSA-PKCS1-v1_5 with SHA-384
- RSASSA-PKCS1-v1_5 with SHA-512
- RSASSA-PSS with SHA-256
- RSASSA-PSS with SHA-384
- RSASSA-PSS with SHA-512

In addition, the CA MAY use `RSASSA-PKCS1-v1_5 with SHA-1` if one of the following conditions are met:

- It is used within Timestamp Authority Certificate and the date of the `notBefore` field is not greater than 2022-04-30; or,
- It is used within an OCSP response; or,
- It is used within a CRL; or,
- It is used within a Timestamp Token and the date of the `genTime` field is not greater than 2022-04-30.

7.1.3.2.2 ECDSA

The CA SHALL use one of the following signature algorithms:

- ECDSA with SHA-256
- ECDSA with SHA-384
- ECDSA with SHA-512

7.1.3.2.3 DSA

The CA SHALL use the following signature algorithm:

- DSA with SHA-256

In addition, the CA MAY use `DSA with SHA-1` if one of the following conditions are met:

- It is used within Timestamp Authority Certificate and the date of the `notBefore` field is not greater than 2022-04-30; or,
- It is used within an OCSP response; or,
- It is used within a CRL; or,
- It is used within a Timestamp Token and the date of the `genTime` field is not greater than 2022-04-30.

7.1.4 Name forms

7.1.4.1 Name encoding

The following requirements SHOULD be met by all newly-issued Subordinate CA Certificates that are not used to issue TLS certificates, as defined in Section 7.1.2.2, and MUST be met for all other Certificates, regardless of whether the Certificate is a CA Certificate or a Subscriber Certificate.

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

7.1.4.2.1 Subject alternative name extension

No stipulation.

7.1.4.2.2 Subject distinguished name fields - EV and Non-EV Code Signing Certificates

a. **Certificate Field:** `subject:commonName` (OID 2.5.4.3)
Required/Optional: Required
Contents: This field MUST contain the Subject's legal name as verified under Section 3.2.2 or 3.2.3.

b. **Certificate Field:** `subject:organizationalUnitName` (OID 2.5.4.11)
Required/Optional: Optional
Contents: The CA MUST implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2.

c. **Certificate Field:** `subject:domainComponent` (OID 0.9.2342.19200300.100.1.25)
Required/Optional: Prohibited
Contents: This field MUST not be present in a Code Signing Certificate.

d. **Certificate Field:** Other subject attributes
Required/Optional: Optional **Contents:** Other attributes MAY be present within the subject field. If present, other attributes MUST contain information that has been verified by the CA. Subject attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.2.3 Subject distinguished name field - Non-EV Code Signing Certificates

a. **Certificate Field:** `subject:organizationName` (OID 2.5.4.10)
Required/Optional: Required
Contents: The `subject:organizationName` field MUST contain either the Subject's name or DBA as verified under BR Section 3.2. 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". Because subject name attributes for individuals (e.g. `subject:givenName` (2.5.4.42) and `subject:surname` (2.5.4.4)) are not broadly supported by application software, the CA MAY use the `subject:organizationName` field to convey a natural person Subject's name or DBA. The CA MUST have a documented process for verifying that the information included in the `subject:organizationName` field is not misleading to a Relying Party.

b. **Certificate Field:** `subject:streetAddress` (OID: 2.5.4.9)
Required/Optional: Optional

Contents: If present, the subject:streetAddress field MUST contain the Subject's street address information as verified under BR Section 3.2.2.1 or 3.2.3.

c. **Certificate Field:** `subject:localityName` (OID: 2.5.4.7)
Required/Optional: Required if the `subject:stateOrProvinceName` field is absent. Optional if the `subject:stateOrProvinceName` field is present.
Contents: If present, the `subject:localityName` field MUST contain the Subject's locality information as verified under BR Section 3.2. If the `subject:countryName` field specifies the ISO 3166-1 user-assigned code of XX in accordance with BR Section 7.1.4.2.2.h., the `subject:localityName` field MAY contain the Subject's locality and/or state or province information as verified under BR Section 3.2.2.1 or 3.2.3.

d. **Certificate Field:** `subject:stateOrProvinceName` (OID: 2.5.4.8)
Required/Optional: Required if the `subject:localityName` field is absent. Optional if the `subject:localityName` field is present.
Contents: If present, the `subject:stateOrProvinceName` field MUST contain the Subject's state or province information as verified under BR Section 3.2.2.1 or 3.2.3. If the `subject:countryName` field specifies the ISO 3166-1 user-assigned code of XX in accordance with BR Section 7.1.4.2.2.h., the `subject:stateOrProvinceName` field MAY contain the full name of the Subject's country information as verified under BR Section 3.2.2.1 or 3.2.3.

e. **Certificate Field:** `subject:postalCode` (OID: 2.5.4.17)
Required/Optional: Optional
Contents: If present, the `subject:postalCode` field MUST contain the Subject's zip or postal information as verified under BR Section 3.2.2.1 or 3.2.3.

f. **Certificate Field:** `subject:countryName` (OID: 2.5.4.6)
Required/Optional: Required
Contents: The `subject:countryName` MUST contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under BR Section 3.2.2.3. If a Country is not represented by an official ISO 3166-1 country code, the CA MAY specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

7.1.4.2.4 Subject distinguished name fields - EV Code Signing Certificates

a. **Certificate Field:** `subject:organizationName` (OID 2.5.4.10)
Required/Optional: Required
Contents: This field MUST contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein. A CA MAY abbreviate the organization prefixes or suffixes in the organization name, e.g., if the official record shows "Company Name Incorporated" the CA MAY include "Company Name, Inc."

When abbreviating a Subject's full legal name as allowed by this subsection, the CA MUST use abbreviations that are not misleading in the Jurisdiction of Incorporation or Registration.

In addition, an assumed name or DBA name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis.

If the combination of names or the organization name by itself exceeds 64 characters, the CA MAY abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that the CA checks this field in accordance with the High Risk Certificate Request requirements of Section 4.2.1 and a Relying Party will not be misled into thinking that they are dealing with a different organization. In cases where this is not possible, the CA MUST NOT issue the EV Code Signing Certificate.

b. **Certificate Field:** `subject:businessCategory` (OID 2.5.4.15)
Required/Optional: Required
Contents: This field MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of Section 4.1.1.1, Section 4.1.1.2, Section 4.1.1.3 or Section 4.1.1.4, respectively.

c. **Certificate Field:** Subject Jurisdiction of Incorporation or Registration Fields

Required/Optional: Required

Certificate Fields:

- Locality (if required): `subject:jurisdictionLocalityName` (OID: 1.3.6.1.4.1.311.60.2.1.1)
- State or province (if required): `subject:jurisdictionStateOrProvinceName` (OID: 1.3.6.1.4.1.311.60.2.1.2)
- Country: `subject:jurisdictionCountryName` (OID: 1.3.6.1.4.1.311.60.2.1.3)

Contents: These fields MUST NOT contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. For example, the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level MUST include the country information but MUST NOT include the state or province or locality information. Similarly, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information, but MUST NOT include locality information. And, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information. Country information MUST be specified using the applicable ISO country code. State or province or locality information (where applicable) for the Subject's Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction.

Effective as of 15 March 2025, the CA SHALL ensure that, at time of issuance, the values within these fields have been disclosed within the latest publicly-available disclosure, as described in Section 3.2.10, as acceptable values for the applicable Incorporating Agency or Registration Agency.

d. **Certificate Field:** `subject:serialNumber` (2.5.4.5)
Required/Optional: Required
Contents:

- For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.

- For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
- For Business Entities, the Registration Number that was received by the Business Entity upon government registration SHALL be entered in this field. For those Business Entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration SHALL be entered into this field in any one of the common date formats.

Effective as of 15 March 2025, if the CA has disclosed a set of acceptable format or formats for Registration Numbers for the applicable Registration Agency or Incorporating Agency, as described in Section 3.2.10, the CA MUST ensure, prior to issuance, that the Registration Number is valid according to at least one currently disclosed format for that applicable Registration Agency or Incorporating agency.

e. **Certificate Field:** Subject Physical Address of Place of Business Fields
Required/Optional: As stated in Section 7.1.4.2 b, c, d, e and f.
Contents: This field MUST contain the address of the physical location of the Subject's Place of Business.

7.1.5 Name constraints

7.1.6 Certificate policy object identifier

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

7.1.6.1 Reserved Certificate Policy Identifiers

The following Certificate Policy Identifier is reserved for use by CAs as a required means of asserting compliance with these Requirements for Non-EV Code Signing Certificates:

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(4) code signing(1)} (2.23.140.1.4.1)`

The following Certificate Policy Identifier is reserved for use by CAs as a required means of asserting compliance with these Requirements for EV Code Signing Certificates follows:

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(3)} (2.23.140.1.3)`

The following Certificate Policy Identifier is reserved for use by CAs as a required means of asserting compliance with these Requirements for Timestamp Certificates:

`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(4) timestamping(2)} (2.23.140.1.4.2)`

7.1.6.2 Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

7.1.6.3 Subordinate CA Certificates

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

1. MUST include the policy identifier that indicates the Subordinate CA's adherence to and compliance with these Requirements (i.e. either the CA/Browser Forum reserved identifiers as specified in Section 7.1.6.1 or identifiers defined by the CA in its Certificate Policy and/or Certification Practice Statement), and
2. MUST NOT contain the "anyPolicy" identifier (`2.5.29.32.0`).

A Certificate issued to a Subordinate CA that issues Code Signing Certificates and is an Affiliate of the Issuing CA:

1. MUST include the CA/Browser Forum reserved identifier specified in Section 7.1.6.1 to indicate the Subordinate CA's compliance with these Requirements, and
2. MAY contain the "anyPolicy" identifier (`2.5.29.32.0`) in place of an explicit policy identifier.

A Certificate issued after 31 March 2022 to a Subordinate CA that issues Timestamp Certificates and is an Affiliate of the Issuing CA:

1. MUST include the CA/Browser Forum reserved identifier specified in Section 7.1.6.1 to indicate the Subordinate CA's compliance with these Requirements, and
2. MAY contain the "anyPolicy" identifier (`2.5.29.32.0`) in place of an explicit policy identifier.

A Subordinate CA MUST represent, in its Certificate Policy and/or Certification Practice Statement, 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 MUST contain one or more policy identifier(s), defined by the CA, in the Certificate's certificatePolicies extension that indicates adherence to and compliance with these Requirements. CAs complying with these Requirements MAY also assert the reserved policy OIDs in such Certificates.

The CA MUST document in its Certificate Policy or Certification Practice Statement that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Requirements.

7.1.7 Usage of Policy Constraints extension

7.1.8 Policy qualifiers syntax and semantics

7.1.9 Processing semantics for the critical Certificate Policies extension

7.2 CRL profile

The serial number of a revoked Certificate MUST remain on the CRL for at least 10 years after the expiration of the Certificate. Application Software Suppliers MAY require the CA to support a longer life-time in its contract with the CA. If a Code Signing Certificate contains the Lifetime Signing OID, the Code Signature becomes invalid when the Code Signing Certificate expires, even if the Code Signature is timestamped. Because the Lifetime Signing OID is intended to be used with test purposes only, a CA MAY cease maintaining revocation information for a Code Signing Certificate with the Lifetime Signing OID after the Code Signing Certificate expires.

If a Code Signing Certificate previously has been revoked, and the CA later becomes aware of a more appropriate revocation date, then the CA MAY use that revocation date in subsequent CRL entries for that Code Signing Certificate.

7.2.1 Version number(s)

7.2.2 CRL and CRL entry extensions

If a CRL has a `thisUpdate` field value of 2022-07-01 00:00:00 UTC or later and the CA includes the Invalidity Date CRL entry extension in a CRL entry for a Code Signing Certificate, then the time encoded in the Invalidity Date CRL extension SHALL be equal to the time encoded in the `revocationDate` field of the CRL entry.

7.3 OCSP profile

If a Code Signing Certificate previously has been revoked, and the CA later becomes aware of a more appropriate revocation date, then the CA MAY use that revocation date in subsequent OCSP responses for that Code Signing Certificate.

7.3.1 Version number(s)

7.3.2 OCSP extensions

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CA and/or all Signing Services MUST, at all times:

1. Comply with all laws applicable to its business and the Certificates it issues in each jurisdiction where it operates,
2. Comply with these Requirements,
3. Comply with the audit requirements set forth in this section, and
4. If a CA, 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.
5. In all cases, the CA MUST contractually obligate each Delegated Third Party to comply with all applicable requirements in these Requirements and to perform them as required of the CA itself. The CA MUST enforce these obligations and internally audit each Delegated Third Party's compliance with these Requirements on an annual basis.

8.1 Frequency or circumstances of assessment

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

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

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

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 Code Signing Certificates, the CA MUST 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 MUST be completed no earlier than twelve (12) months prior to issuing Code Signing Certificates and MUST be followed by a complete audit under such scheme within ninety (90) days of issuing the first Code Signing Certificate.

Audits MUST be conducted for all obligations under these Guidelines, including the operations of Timestamp Authorities and Signing Services. Functions performed by a Delegated Third Party MUST be included in the CA's audit or the CA MUST obtain an audit report from the Delegated Third Party. If the opinion is that the Delegated Third Party does not comply, then the CA MUST not allow the Delegated Third Party to continue performing delegated functions.

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

8.2 Identity/qualifications of assessor

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

1. Independence from the subject of the audit;

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

8.3 Assessor's relationship to assessed entity

8.4 Topics covered by assessment

8.4.1 CA assessment

The CA MUST undergo a conformity assessment audit for compliance with these Requirements performed in accordance with one of the following schemes:

1. "WebTrust for CAs v2.0 or newer" AND "WebTrust for Certification Authorities – Code Signing Baseline Requirements v2.0 or newer" AND "WebTrust for Certification Authorities – Network Security – Version 1.0 or newer"; or
2. ETSI EN 319 411-1, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied); or
3. If a government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either (a) encompasses all requirements of one of the above schemes or (b) consists of comparable criteria that are available for public review.

Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Auditor, as specified in Section 8.2.

The audit MUST cover all CA obligations under these Guidelines regardless of whether they are performed directly by the CA, an RA, or subcontractor.

8.4.2 Signing Service assessment

For Audit Periods starting after June 30, 2024, the Signing Service MUST undergo a conformity assessment audit for compliance with these Requirements performed in accordance with one of the following schemes:

1. "WebTrust for Certification Authorities – Code Signing Baseline Requirements v2.0 or newer" AND "WebTrust for Certification Authorities – Network Security – Version 1.0 or newer"; or
2. ETSI EN 319 411-1, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied).

Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability

procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Auditor, as specified in BR Section 8.2.

8.4.3 Timestamp Authority assessment

The Timestamp Authority MUST undergo a conformity assessment audit for compliance with these Requirements performed in accordance with one of the following schemes:

1. "WebTrust for Certification Authorities – Code Signing Baseline Requirements v2.0 or newer" AND "WebTrust for Certification Authorities – Network Security – Version 1.0 or newer"; or
2. ETSI EN 319 411-1, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied).

Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Auditor, as specified in BR Section 8.2.

8.5 Actions taken as a result of deficiency

8.6 Communication of results

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

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

The Audit Report MAY combine the results of the assessments defined in Section 8.4, if the assessments were performed by the same Qualified Auditor.

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

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

11. (for audits conducted in accordance with any of the ETSI standards) a statement to indicate that the auditor referenced the applicable CA/Browser Forum criteria, such as this document, and the version used.

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

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

8.7 Self-audits

CAs must abide by the self-audit requirements of these Guidelines. During the period in which it issues Code Signing Certificates, the CA MUST strictly control its service quality by performing ongoing self-audits against a randomly selected sample of at least three percent of the Non-EV Code Signing Certificates and at least three percent of the EV Code Signing Certificates it has issued in the period beginning immediately after the last sample was taken. For all Code Signing Certificates where the final cross-correlation and due diligence requirements of Section 8 of these Guidelines is performed by an RA, the CA MUST strictly control its service quality by performing ongoing self-audits against a randomly selected sample of at least six percent of the Non-EV Code Signing Certificates and at least six percent of the EV Code Signing Certificates it has issued in the period beginning immediately after the last sample was taken.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

9.1.2 Certificate access fees

9.1.3 Revocation or status information access fees

9.1.4 Fees for other services

9.1.5 Refund policy

9.2 Financial responsibility

9.2.1 Insurance coverage

For EV Code Signing Certificates, the CA SHALL maintain the following insurance related to their respective performance and obligations under these Guidelines:

1. Commercial General Liability insurance (occurrence form) with policy limits of at least two million US dollars in coverage; and
2. Professional Liability/Errors and Omissions insurance, with policy limits of at least five million US dollars in coverage, and including coverage for:
    1. claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Code Signing Certificates, and;
    2. claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

Such insurance must be with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated).

A CA MAY self-insure for liabilities that arise from such party's performance and obligations under these Guidelines provided that it has at least five hundred million (500.000.000) US dollars in liquid assets based on audited financial statements in the past twelve months, and a quick ratio (ratio of liquid assets to current liabilities) of not less than 1.0.

9.2.2 Other assets

9.2.3 Insurance or warranty coverage for end-entities

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

9.3.2 Information not within the scope of confidential information

9.3.3 Responsibility to protect confidential information

9.4 Privacy of personal information

9.4.1 Privacy plan

9.4.2 Information treated as private

9.4.3 Information not deemed private

9.4.4 Responsibility to protect private information

9.4.5 Notice and consent to use private information

9.4.6 Disclosure pursuant to judicial or administrative process

9.4.7 Other information disclosure circumstances

9.5 Intellectual property rights

9.6 Representations and warranties

9.6.1 CA representations and warranties

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

1. **Compliance**. The CA and any Delegated Third Party each represents that it has complied with these Requirements and the applicable Certificate Policy and Certification Practice Statement in issuing each Code Signing Certificate and operating its PKI or delegated service.
2. **Legal Existence**: For EV Code Signing Certificates, the CA has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Code Signing Certificate was issued, the Subject of the EV Code Signing Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration.
3. **Identity of Subscriber**: At the time of issuance, the CA represents that it (i) operated a procedure for verifying the identity of the Subscriber that at least meets the requirements in Section 3.2 of this document, (ii) followed the procedure when issuing or managing the Certificate, and (iii) accurately described the same procedure in the CA's Certificate Policy or Certification Practice Statement.
4. **Authorization for Certificate:** At the time of issuance, the CA represents that it (i) operated a procedure for verifying that the Applicant authorized the issuance of the Certificate, (ii) followed the procedure, and (iii) accurately described the same procedure in the CA's Certificate Policy or Certification Practice Statement.
5. **Accuracy of Information:** At the time of issuance, the CA represents that it (i) operated a procedure for verifying that all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute) was true and accurate, (ii) followed the procedure, and (iii) accurately described the same procedure in the CA's Certificate Policy or Certification Practice Statement.
6. **Key Protection:** The CA represents that it provided the Subscriber at the time of issuance with documentation on how to securely store and prevent the misuse of Private Keys associated with Code Signing Certificates, or in the case of a Signing Service, securely stored and prevented the misuse of Private Keys associated with Code Signing Certificates;

7. **Subscriber Agreement:** The CA represents that the CA entered into a legally valid and enforceable Subscriber Agreement with the Applicant that satisfies these Requirements or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use.
8. **Status:** The CA represents that it will maintain a 24 x 7 online-accessible Repository with current information regarding the status of Certificates as valid or revoked for the period required by these Requirements.
9. **Revocation:** The CA represents that it will revoke a Certificate upon the occurrence of a revocation event specified in these Requirements.

9.6.2 RA representations and warranties

9.6.3 Subscriber representations and warranties

The CA MUST require, as part of the Subscriber Agreement, that the Applicant make the commitments and warranties set forth in this section, as applicable, for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either: 1. The Applicant's agreement to the Subscriber Agreement with the CA, or 2. The Applicant's acknowledgement of the Terms of Use.

The CA SHALL implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use. The Subscriber Agreement or Terms of Use MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information:** To provide accurate and complete information at all times in connection with the issuance of a Certificate, including in the Certificate Request and as otherwise requested by the CA.
2. **Protection of Private Key:** Where the key is available outside a Signing Service, to maintain sole control of, keep confidential, and properly protect, at all times in accordance with Section 6.2.7.4, the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token). The CA MUST provide the Subscriber with documentation on how to protect a Private Key. The CA MAY provide this documentation as a white paper or as part of the Subscriber Agreement. The Subscriber MUST represent that it will generate and operate any device storing Private Keys in a secure manner, as described in a document of code signing best practices, which the CA MUST provide to the Subscriber during the ordering process. The CA MUST obligate the Subscriber to use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport Private Keys.
3. **Private Key Reuse:** To not apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate.
4. **Use:** To use the Certificate and associated Private Key only for authorized and legal purposes,

including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.

5. **Compliance with Industry Standards**: An acknowledgment and acceptance that the CA may modify the Subscriber Agreement or Terms of Use when necessary to comply with any changes in these Requirements or the Baseline Requirements.
6. **Prevention of Misuse:** To provide adequate network and other security controls to protect against misuse of the Private Key and that the CA will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys.
7. **Acceptance of Certificate:** Not to use the Certificate until after the Applicant, or an agent of Applicant, has reviewed and verified the Certificate contents for accuracy.
8. **Reporting and Revocation:** To promptly cease using a Certificate and its associated Private Key and promptly request that the CA revoke the Certificate if the Subscriber believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused or compromised, or (c) there is evidence that the Certificate was used to sign Suspect Code.
9. **Sharing of Information**: An acknowledgment and acceptance that, if: (a) the Certificate or the Applicant is identified as a source of Suspect Code, (b) the authority to request the Certificate cannot be verified, or (c) the Certificate is revoked for reasons other than Subscriber request (e.g. as a result of Private Key compromise, discovery of malware, etc.), then the CA is authorized to share information about the Applicant, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.
10. **Termination of Use of Certificate:** To promptly cease using the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of the Certificate.
11. **Responsiveness:** An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
12. **Acknowledgment and Acceptance:** An acknowledgement and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the Terms of Use or the Subscriber Agreement.

9.6.4 Relying party representations and warranties

9.6.5 Representations and warranties of other participants

The CA MUST contractually obligate each Signing Service to inform the CA if the Signing Service becomes aware (by whatever means) that the Signing Service has signed Suspect Code. The CA MUST require the Signing Service to request revocation of the affected Certificate and provide immediate notice to the CA if a Subscriber's Private Key, or Private Key activation data, is compromised or believed to be compromised. The CA MUST revoke the affected Certificate upon request by the Signing Service or if the CA determines the Signing Service failed to notify the CA within 24 hours after identifying a Key compromise.

Signing Services MUST obtain the Subscriber's commitment to:

1. Use such signing services solely for authorized purposes that comply with the Subscriber Agreement/Terms of Use, these Requirements, and all applicable laws,
2. Not knowingly submit software for Code Signature that contains Suspect Code, and
3. Inform the Signing Service if it is discovered (by whatever means) that Code submitted to the Signing Service for Code Signature contained Suspect Code

9.7 Disclaimers of warranties

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.

For Non-EV Code Signing Certificates, the CA MAY disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in the CA's Certificate Policy and/or Certification Practice Statement. If the CA has not issued or managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA MAY seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that the CA desires. If the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement, then the CA SHALL include the limitations on liability in the CA's Certificate Policy and/or Certification Practice Statement.

For EV Code Signing Certificates, CAs MAY limit their liability as described in this Section 9.8 for Non-EV Code Signing Certificates, but MUST NOT limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than two thousand US dollars per Subscriber or Relying Party per EV Code Signing Certificate.

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

9.10.2 Termination

9.10.3 Effect of termination and survival

9.11 Individual notices and communications with participants

9.12 Amendments

9.12.1 Procedure for amendment

9.12.2 Notification mechanism and period

9.12.3 Circumstances under which OID must be changed

9.13 Dispute resolution provisions

9.14 Governing law

9.15 Compliance with applicable law

9.16 Miscellaneous provisions

9.16.1 Entire agreement

9.16.2 Assignment

9.16.3 Severability

If a court or government body with jurisdiction over the activities covered by these Requirements determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved MUST notify the CA/Browser Forum of the facts, circumstances, and law(s) involved.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

9.16.5 Force Majeure

9.17 Other provisions

Appendix A High risk regions of concern

The geographic locations listed below have more than 5% of the Code Signing Certificates for that location associated with signed Suspect Code when compared to the number of all Code Signing Certificates for that area. Applications originating or associated from one of these HRRCs are considered high risk and require additional verification as specified under Section 4.2.2 of this document:

NONE

Appendix B - Sample Attorney Opinions Confirming Specified Information

(Informative)

[Law Firm Letterhead]

[Date]

To:	**(Name of Issuing Certification Authority)(Address / fax number of Issuing CA – may be sent by fax or email attachment)**
Re:	**EV Code Signing Certificate Request No. (CA Reference Number)**
Client:	**(Exact company name of Client – see footnote 1)**
Client Representative:	**(Exact name of Client Representative who signed the Application – see footnote 2)**
Application Date:	**(Insert date of Client's Application to the Issuing CA)**

This firm represents *[**exact** company name of Client]* [3] ("Client"), who has submitted the Application to you dated as of the Application Date shown above ("Application"). We have been asked by our Client to present you with our opinion as stated in this letter.

[Insert customary preliminary matters for opinion letters in your jurisdiction.]

On this basis, we hereby offer the following opinion:

1. That [exact company name of Client] ("Company") is a duly formed [corporation, LLC, etc.] that is "active," "valid," "current," or the equivalent under the laws of the state/province of [name of governing jurisdiction where Client is incorporated or registered] and is not under any legal disability known to the author of this letter.
2. That Company conducts business under the assumed name or "DBA"*[assumed name of the Applicant]* and has registered such name with the appropriate government agency in the jurisdiction of its place of business below.
3. That *[name of Client's Representative]*[4] has authority to act on behalf of Company to: [*select as appropriate*] (a) provide the information about Company required for issuance of the EV Code Signing Certificates as contained in the attached Application, (b) request one or more EV Code Signing Certificates and to designate other persons to request EV Code Signing Certificates, and (c) agree to the relevant contractual obligations contained in the Subscriber Agreement on behalf of Company.
4. That Company has a physical presence and its place of business is at the following location:

   _____ _____ _____
5. That Company can be contacted at its stated place of business at the following telephone number:

[3] This must be the Client's exact corporate name, as registered with the relevant Incorporating Agency in the Client's Jurisdiction of Incorporation. This is the name that will be included in the EV Code Signing Certificate.

[4] If necessary to establish the Client Representative's actual authority, you may rely on a Power of Attorney from an officer of Client who has authority to delegate the authority to the Client Representative.

_____

6. That Company has an active current Demand Deposit Account with a regulated financial institution.
7. That Company has the right to use the following Domain Name in identifying itself on the Internet:

   _____

Insert customary limitations and disclaimers for opinion letters in your jurisdiction.

(Name and signature)

[Jurisdiction(s) in which attorney / Latin notary is admitted to practice][5]

cc: [Send copy to Client_]_

[5]This letter may be issued by in-house counsel for the Client so long as permitted by the rules of your jurisdiction.

Appendix C - Sample Accountant Letters Confirming Specified Information

(Informative)

It is acceptable for professional accountants to provide letters that address specified matters. The letters would be provided in accordance with the professional standards in the jurisdiction in which the accountant practices.

Two examples of the letter that might be prepared by an accountant in the United States and in Canada follow:

UNITED STATES

To the [Certification Authority] and Management of [Client]:

We have performed the procedures enumerated below, which were agreed to by the Managements of Client, solely to assist you in evaluating the company's application for an Extended Validation (EV) Certificate, dated....., 20..... This agreed-upon procedures engagement was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. The sufficiency of these procedures is solely the responsibility of those parties specified in this report. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

Specified Information:	Procedure:(Note 1: These are illustrative of the procedures that would be undertaken and are designed to meet the needs of the Certification Authorities issuing Extended Validation Certificates)	Results: (Note 2: If you are unavailable to perform any of the stated procedure, this should be noted in this column. Any exceptions should be noted in a separate paragraph below)
Legal Name - 123456 Delaware corporation	Agree legal name to permanent audit file information (If audit has been completed).	Legal name on the application agrees with the information contained in our permanent file with respect to Client.(If there is no permanent file, state this fact)
Doing business as - "Name"	Agree name to government data base of business names	The name "Name" is registered with the (name of database to which the name was agreed)
Physical location - "Address Information"	Visit the location at the address	Site visit completed at Address
Business Phone Number - 555 999 9999	Phone the number provided and confirm that it was answered by the named organization	Phoned Business Number and noted that it was answered with the Doing Business As name. This would provided by the receptionist

Specified Information:	Procedure:(Note 1: These are illustrative of the procedures that would be undertaken and are designed to meet the needs of the Certification Authorities issuing Extended Validation Certificates)	Results: (Note 2: If you are unavailable to perform any of the stated procedure, this should be noted in this column. Any exceptions should be noted in a separate paragraph below)
Bank Account – "Bank Name", "Account Number"	Request a letter directly from "the Bank" confirming the existence of the account for the benefit of "the Client"	Received letter directly from "the Bank" confirming the existence of the account for the benefit of "the Client"
The corporate officers are "NAMED" (verified officer)	Agree Names to annual shareholders meeting minutes (Note - not required to personally know the officers)	Agreed Names listed as corporate officers on the application to minute books maintained by the Client
Name of application signer and approver	Obtain letter from verified Officer confirming the names of the application signer and approver	Obtained letter from the President confirming the names of the duly authorized names of the application signer and approver as they appear in the application

We were not engaged to and did not conduct an examination, the objective of which would be the expression of an opinion on the Application for Extended Validation Certificate. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended solely for the information and use of the Certification Authority and managements of Client, and is not intended to be and should not be used by anyone other than these specified parties.

[Signature]

[Date]

CANADA

To: [Name of Certification Authority]

Re: Client Limited [Applicant]

As specifically agreed, I/we have performed the following procedures in connection with the above company's application for an Extended Validation (EV) Certificate, dated ....., 20.... with respect to the following specified information contained in the application

Specified Information:	Procedure:(Note 1: These are illustrative of the procedures that would be undertaken and are designed to meet the needs of the Certification Authorities issuing Extended Validation Certificates)	Results: (Note 2: If you are unavailable to perform any of the stated procedure, this should be noted in this column. Any exceptions should be noted in a separate paragraph below)

Specified Information:	Procedure:(Note 1: These are illustrative of the procedures that would be undertaken and are designed to meet the needs of the Certification Authorities issuing Extended Validation Certificates)	Results: (Note 2: If you are unavailable to perform any of the stated procedure, this should be noted in this column. Any exceptions should be noted in a separate paragraph below)
Legal Name - 123456 Ontario limited	Agree legal name to permanent audit file information (If audit has been completed)	Legal name on the application agrees with the information contained in our permanent file with respect to Client.(If there is no permanent file, state this fact)
Doing business as - "Name"	Agree name to government data base of business names	The name "Name" is registered with the (name of database to which the name was agreed)
Physical location - "Address Information"	Visit the location at the address	Site visit completed at Address
Business Phone Number - 555 999 9999	Phone the number provided and confirm that it was answered by the named organization	Phoned Business Number and noted that it was answered with the Doing Business As name. This would provided by the receptionist
Bank Account – "Bank Name", "Account Number"	Request a letter directly from "the Bank" confirming the existence of the account for the benefit of "the Client"	Received letter directly from "the Bank" confirming the existence of the account for the benefit of "the Client"
The corporate officers are "NAMED" (verified officer)	Agree Names to annual shareholders meeting minutes (Note - not required to personally know the officers)	Agreed Names listed as corporate officers on the application to minute books maintained by the Client
Name of application signer and approver	Obtain letter from verified Officer confirming the names of the application signer and approver	Obtained letter from the President confirming the names of the duly authorized names of the application signer and approver as they appear in the application

As a result of applying the above procedures, I/we found [no / the following] exceptions [list of exceptions]. However, these procedures do not constitute an audit of the company's application for an EV Code Signing Certificate, and therefore I express no opinion on the application dated ....., 20.....

This letter is for use solely in connection with the application for an Extended Validation Certificate by [Client] dated ....., 20.....

City

(signed) .....

Appendix D - Country-Specific Interpretative Guidelines (Normative)

NOTE: This appendix provides alternative interpretations of Requirements related to EV Code Signing Certificates, for countries that have a language, cultural, technical, or legal reason for deviating from a strict interpretation of these Requirements. More specific information for particular countries may be added to this appendix in the future.

1. Organization Names

1. Non-Latin Organization Name

   Where an EV Applicant's organization name is not registered with a QGIS in *Latin* characters and the Applicant's foreign character organization name and registration have been verified with a QGIS in accordance with these Guidelines, a CA MAY include a Latin character organization name in the EV Code Signing Certificate. In such a case, the CA MUST follow the procedures laid down in this section.

2. Romanized Names

   In order to include a transliteration/Romanization of the registered name, the Romanization MUST be verified by the CA using a system officially recognized by the Government in the Applicant's Jurisdiction of Incorporation.

   If the CA can not rely on a transliteration/Romanization of the registered name using a system officially recognized by the Government in the Applicant's Jurisdiction of Incorporation, then it MUST rely on one of the options below, in order of preference:

   1. A system recognized by the International Organization for Standardization (ISO);
   2. A system recognized by the United Nations; or
   3. A Lawyer's Opinion or Accountant's Letter confirming the proper Romanization of the registered name.

3. Translated Name

   In order to include a Latin character name in the EV certificate that is not a direct Romanization of the registered name (e.g. an English Name) the CA MUST verify that the Latin character name is:

   1. Included in the Articles of Incorporation (or equivalent document) filed as part of the organization registration; or
   2. Recognized by a QTIS in the Applicant's Jurisdiction of Incorporation as the Applicant's recognized name for tax filings; or
   3. Confirmed with a QIIS to be the name associated with the registered organization; or
   4. Confirmed by a Verified Legal Opinion or Accountant's Letter to be a translated trading name associated with the registered organization.

Country-Specific Procedures

D-1. Japan

As interpretation of the procedures set out above:

1. Organization Names

1. The Revised Hepburn method of Romanization, as well as Kunrei-shiki and Nihon-shiki methods described in ISO 3602, are acceptable for Japanese Romanizations.
2. The CA MAY verify the Romanized transliteration, language translation (e.g. English name), or other recognized Roman-letter substitute of the Applicant's formal legal name with either a QIIS, Verified Legal Opinion, or Verified Accountant Letter.
3. The CA MAY use the Financial Services Agency to verify a Romanized, translated, or other recognized Roman-letter substitute name. When used, the CA MUST verify that the translated English is recorded in the audited Financial Statements.
4. When relying on Articles of Incorporation to verify a Romanized, translated, or other recognized Roman-letter substitute name, the Articles of Incorporation MUST be accompanied either: by a document, signed with the original Japanese Corporate Stamp, that proves that the Articles of Incorporation are authentic and current, or by a Verified Legal Opinion or a Verified Accountant Letter. The CA MUST verify the authenticity of the Corporate Stamp.
5. A Romanized, translated, or other recognized Roman-lettered substitute name confirmed in accordance with this Appendix D-1 stored in the ROBINS database operated by JIPDEC MAY be relied upon by a CA for determining the allowed organization name during any issuance or renewal process of an EV Code Signing Certificate without the need to re-perform the above procedures.

2. Accounting Practitioner

   In Japan:

   1. Accounting Practitioner includes either a certified public accountant (公認会計士 - Konin-kaikei-shi) or a licensed tax accountant (税理士 – Zei-ri-shi).
   2. The CA MUST verify the professional status of the Accounting Practitioner through direct contact with the relevant local member association that is affiliated with either the Japanese Institute of Certified Public Accountants (http://www.hp.jicpa.or.jp), the Japan Federation of Certified Tax Accountant's Associations (http://www.nichizeiren.or.jp), or any other authoritative source recognized by the Japanese Ministry of Finance (http://www.mof.go.jp) as providing the current registration status of such professionals.

3. Legal Practitioner

   In Japan:

   1. Legal Practitioner includes any of the following:

      - a licensed lawyer (弁護士 - Ben-go-shi),
      - a judicial scrivener (司法書士 - Shiho-sho-shi lawyer),
      - an administrative solicitor (行政書士 - Gyosei-sho-shi Lawyer),
      - or a notary public (公証人 - Ko-sho-nin).

      For purposes of the EV Guidelines, a Japanese Notary Public is considered equivalent to a Latin Notary.

   2. The CA MUST verify the professional status of the Legal Practitioner by direct contact through the relevant local member association that is affiliated with one of the following national associations:

      - the Japan Federation of Bar Associations (http://www.nichibenren.or.jp),

- the Japan Federation of Shiho-Shoshi Lawyer's Associations (http://www.shiho-shoshi.or.jp),
- the Japan Federation of Administrative Solicitors (http://www.gyosei.or.jp),
- the Japan National Notaries Association (http://www.koshonin.gr.jp), or
- any other authoritative source recognized by the Japanese Ministry of Justice (http://www.moj.go.jp) as providing the current registration status of such professionals.

Appendix E - Sample Contract Signer's Representation/Warranty (Informative)

A CA may rely on the Contract Signer's authority to enter into the Subscriber Agreement using a representation/warranty executed by the Contract Signer. An example of an acceptable warranty is as follows:

[CA] and Applicant are entering into a legally valid and enforceable Subscriber Agreement that creates extensive obligations on Applicant. An EV Code Signing Certificate serves as a form of digital identity for Applicant. The loss or misuse of this identity can result in great harm to the Applicant. By signing this Subscriber Agreement, the contract signer acknowledges that they have the authority to obtain the digital equivalent of a company stamp, seal, or (where applicable) officer's signature to establish the authenticity of the company's website, and that [Applicant name] is responsible for all uses of its EV Code Signing Certificate. By signing this Agreement on behalf of [Applicant name], the contract signer represents that the contract signer

1. is acting as an authorized representative of [Applicant name],
2. is expressly authorized by [Applicant name] to sign Subscriber Agreements and approve EV Code Signing Certificate requests on Applicant's behalf, and
3. has confirmed Applicant's right to use the domain(s) to be included in EV Code Signing Certificates.

Appendix F – Unused

This appendix is intentionally left blank.

Appendix G – Abstract Syntax Notation One module for EV certificates

```
CABFSelectedAttributeTypes {
    joint-iso-itu-t(2) international-organizations(23)
    ca-browser-forum(140) module(4)
    cabfSelectedAttributeTypes(1) 1 }
DEFINITIONS ::=
BEGIN
-- EXPORTS All
IMPORTS
  -- from Rec. ITU-T X.501 | ISO/IEC 9594-2
  selectedAttributeTypes, ID, ldap-enterprise
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
    usefulDefinitions(0) 7}

  -- from the X.500 series
  ub-locality-name, ub-state-name
    FROM UpperBounds {joint-iso-itu-t ds(5) module(1) upperBounds(10) 7}

  -- from Rec. ITU-T X.520 | ISO/IEC 9594-6
  DirectoryString{}, CountryName
    FROM SelectedAttributeTypes selectedAttributeTypes;

id-evat-jurisdiction ID ::= {ldap-enterprise 311 ev(60) 2 1}
id-evat-jurisdiction-localityName ID ::= {id-evat-jurisdiction 1}
id-evat-jurisdiction-stateOrProvinceName ID ::= {id-evat-jurisdiction 2}
id-evat-jurisdiction-countryName ID ::= {id-evat-jurisdiction 3}

jurisdictionLocalityName ATTRIBUTE ::= {
  SUBTYPE OF    name
  WITH SYNTAX   DirectoryString{ub-locality-name}
  LDAP-SYNTAX   directoryString.&id
  LDAP-NAME     {"jurisdictionL"}
  ID            id-evat-jurisdiction-localityName }

jurisdictionStateOrProvinceName ATTRIBUTE ::= {
  SUBTYPE OF    name
  WITH SYNTAX   DirectoryString{ub-state-name}
  LDAP-SYNTAX   directoryString.&id
  LDAP-NAME     {"jurisdictionST"}
  ID            id-evat-jurisdiction-stateOrProvinceName }

jurisdictionCountryName ATTRIBUTE ::= {
  SUBTYPE OF    name
  WITH SYNTAX   CountryName
  SINGLE VALUE  TRUE
  LDAP-SYNTAX   countryString.&id
  LDAP-NAME     {"jurisdictionC"}
```

```
  ID              id-evat-jurisdiction-countryName }

END
```