Version 2.8 (May 6, 2022)

Commented [CB1]: 3.0

Commented [CB2]: TBD

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

Table of Contents

1. Scope

1.1 Overview

Commented [CB3]: Copied to 1.1

The Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates describe a subset of the requirements that a Certification Authority must meet to issue Code Signing Certificates. Except where specifically stated or in the event of conflict in which case these Requirements will prevail, this document incorporates by reference the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements"), the Network and Certificate System Security Requirements and, in the case of EV Code Signing Certificates, the Guidelines For The Issuance And Management of Extended Validation Certificates as established by the CA/Browser Forum, copies of which are available on the CA/Browser Forum's website at www.cabforum.org.

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).

1.2 Revisions

Commented [CB4]: Copied to 1.2.1

Version	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
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	3 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 Private Key Protection	6 May 2022

1.3 Relevant Dates

Commented [CB5]: Copied to 1.2.2 with changes to section numbers

Compliance	Section(s)	Summary Description (See Full Text for Details)
2021-06-01	Appendix A (1)	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	Appendix A (2)	CAs SHALL support minimum RSA-3072 for Timestamp Certificates, Root Certificates and Subordinate CA Certificates. CAs SHALL NOT support SHA-1 digest algorithm for Timestamp Certificates.
2021-06-01	14.1	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	16.2	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.
2021-11-01	11.1.1(4)	The method used to verify the identity of the Certificate Requester SHALL be per section 11.1.2.
2022-03-31	9.3.3	Subordinate CA Certificates issued for Subordinate CA that issues Timestamping Certificates and is an Affiliate of the Issuing CA must include the reserved identifier specified in Section 9.3.1.
2022-04-30	Appendix A (3)	CAs SHALL NOT support SHA-1 digest algorithm for Timestamp tokens.
2022-07-01	13.2.1	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.
2022-11-15	6.2.7.4.2	Effective November, 15, 2022, 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).
2022-11-15	6.2.7.4.2	Effective November, 15, 2022, 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.

2022-11-15	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 November 15, 2022, 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.

2. Purpose

Commented [CB6]: Moved to 1.1

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.

3. References

Commented [CB7]: Moved to 1.6.3

This document references the following CA/Browser Forum documents:

- the Baseline Requirements, version 1.6.9
- the EV Guidelines, version 1.7.2.

Cross-references to Sections of the Baseline Requirements are notated with the letters "BR", as in "BR Section 1.2."

These documents are available on the CA/Browser Forum's website at www.cabforum.org.

4. Definitions

Commented [CB8]: Moved to 1.6.1

Capitalized Terms are as defined in the Baseline Requirements or the EV SSL Guidelines except where defined below:

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.

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

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.

Certificate Beneficiaries: As defined in section 7.1.1.

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, contains the anyExtendedKeyUsage EKU, or omits the EKU extension and is trusted in an Application Software Provider's root store to sign software objects. [NOTE: Appendix B, subsection (3) of Appendix B requires the presence of the codeSigning EKU and prohibits use of the anyExtendedKeyUsage EKU.]

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.

EV Code Signing Certificate: A Code Signing Certificate validated and issued in accordance the EV Code Signing requirements.

EV Guidelines: The CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates.

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 Region of Concern (HRRC): As set forth in Appendix D, 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.

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.

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.

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.

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.

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

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

Requirements: This document, the Baseline Requirements, the Network and Certificate System Security Requirements and the EV SSL Guidelines.

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 signs Code on behalf of a Subscriber using a Private Key associated with a Code Signing Certificate.

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.

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.

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, and 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 Signing Service or 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.

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.

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.

5. Abbreviations and Acronyms

Commented [CB9]: Moved to 1.6.2

As specified in the Baseline Requirements and EV Guidelines or listed below:

6. Conventions

Commented [CB10]: Moved to 1.6.4

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.

7. Certificate Warranties and Representations

7.1 Certificate Beneficiaries

Commented [CB11]: Moved to 1.6.1 as a definition

Certificate Beneficiaries means any one of the following:

1. 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, or
2. All Relying Parties who reasonably rely on such a Certificate while a Code Signature associated with the Certificate is valid.

7.2 Certificate Warranties

Commented [CB12]: 9.6.1

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

1. **Compliance**. The CA and any Signing Service 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 Signing 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 or Signing Service represents that it (i) operated a procedure for verifying the identity of the Subscriber that at least meets the requirements in Section 11 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 and Signing Service represent that the CA or Signing Service 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.

7.3 Applicant Warranty

Commented [CB13]: 9.6.3

The CA or Signing Service MUST require, as part of the Subscriber Agreement, that the Applicant make the commitments and warranties set forth in Section 10.3.2 and/or Section 10.3.3 of this document, as applicable, for the benefit of the CA and the Certificate Beneficiaries.

8. Community and Applicability

8.1 Compliance

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 Section 17 of this document, 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.

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.

8.2 Certificate Policies

8.2.1 Implementation

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.

8.2.2 Disclosure

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.

8.3 Commitment to Comply

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

Commented [CB14]: 8

Commented [CB15]: 9.16.3

Commented [CB16]: 2.2

Commented [CB17]: 2.2

Commented [CB18]: 2.2

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.

8.4 Trust model

Commented [CB19]: 2.2

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).

8.5 Insurance

Commented [CB20]: 9.2.1

For EV Code Signing Certificates, the CA must meet the requirements and abide by the obligation in Section 8.4 of the EV Guidelines.

8.6 Obtaining EV Code Signing Certificates

Commented [CB21]: 4.1.1

For EV Code Signing Certificates, the CA MAY only issue to Applicants that meet the requirements specified in Section 8.5 of the EV Guidelines.

9. Certificate Content and Profile

9.1 Issuer Information

Commented [CB22]: 7.1.4.1

As specified in BR Section 7.1.4.1.

9.2 Subject Information

Code Signing Certificates issued to Subscribers MUST include the following information in the fields listed:

9.2.1 Subject Alternative Name Extension

Commented [CB23]: 7.14.2.1

No Stipulation.

9.2.2 Subject Common Name Field

Commented [CB24]: 7.1.4.2.2 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 Section11.1.1 or 11.2.1.

9.2.3 Subject Domain Component Field

Commented [CB25]: 7.1.4.2.2 c

This field MUST not be present in a Code Signing Certificate.

9.2.4 Subject Distinguished Name Fields for Non-EV Code Signing Certificates

Commented [CB26]: 7.1.4.2.3

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. givenName (2.5.4.42) and 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**: Number and street: 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 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 thesubject: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.

9.2.5 Subject Distinguished Name Fields for EV Code Signing Certificates

Commented [CB27]: 7.1.4.2.4

a. **Certificate Field**: subject:organizationName (OID 2.5.4.10)

As specified in Section 9.2.1 of the EV Guidelines.

b. Certificate Field: subject:businessCategory (OID 2.5.4.15)

As specified in Section 9.2.3 of the EV Guidelines.

c. Subject Jurisdiction of Incorporation or Registration Field

As specified in Section 9.2.4 of the EV Guidelines.

d. **Certificate Field:** subject:serialNumber (2.5.4.5)

As specified in Section 9.2.5 of the EV Guidelines.

e. Subject Physical Address of Place of Business Field

As specified in Section 9.2.6 of the EV Guidelines.

9.2.6 Subject Organizational Unit Field

Commented [CB28]: 7.1.4.2.2 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 11.

9.2.7 Other Subject Attributes

Commented [CB29]: 7.1.4.2.2 d

As specified in BR Section 7.1.4.2.2.j. 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.

9.3 Certificate Policy Identification

Commented [CB30]: 7.1.6

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.

9.3.1 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)

9.3.2 Root CA Requirements

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

9.3.3 Subordinate CA Certificates

A Certificate issued after 31 January 2017 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 9.3.1 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 after 31 January 2017 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 9.3.1 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 Timestamping Certificates and is an Affiliate of the Issuing CA:

1. MUST include the CA/Browser Forum reserved identifier specified in Section 9.3.1 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.

9.3.4 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.

9.4 Maximum Validity Period

Commented [CB31]: 6.3.2

Subscribers and Signing Services MAY sign Code at any point in the development or distribution process. Code Signatures may be verified at any time, including during download, unpacking, installation, reinstallation, or execution, or during a forensic investigation.

The validity period for a Code Signing Certificate issued to a Subscriber or Signing Service 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 "Minimum Cryptographic Algorithm and Key Size Requirements" in Appendix A for the communicated time period.

9.5 Subscriber Public Key

Commented [CB32]: 6.1.1.3

The CA SHALL reject a certificate request if the requested Public Key does not meet the requirements set forth in Appendix A, BR Section 6.1.6 or if it has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

9.6 Certificate Serial Number

Commented [CB33]: 7.1

As specified in BR Section 7.1.

9.7 Reserved

9.8 Reserved

10. Certificate Request

10.1 General Requirements

10.1.1 Documentation Requirements

Commented [CB34]: 4.1.2 and 5.4.1.

As specified in BR Sections 4.1.2 and 5.4.1.

10.1.2 Role Requirements

Commented [CB35]: 3.2.2.2

For EV Code Signing Certificates, roles are specified in EV Guidelines Section 10.1.2.

10.2 Certificate Request

10.2.1 General

Commented [CB36]: 4.1.2

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 11.3, 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.

Prior to signing Code, the Signing Service MUST obtain from the Applicant a signing request in a form prescribed by the Signing Service and that complies with these Requirements. One signing request MAY suffice for multiple Code Signatures for the same Applicant, subject to the requirements specified herein. The signing request MAY be made, submitted and/or signed electronically.

10.2.2 Request and Certification

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

10.2.3 Information Requirements

The certificate request or signing request MAY include all factual information about the Applicant necessary to issue the Certificate or sign the Code, and such additional information as is necessary for the CA or Signing Service 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 or signing request does not contain all the necessary information about the Applicant, the CA or Signing Service 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 or Signing Service MUST establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

10.2.4 Subscriber Private Key

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 either transport the Private Key in hardware with an activation method that is equivalent to 128 bits of encryption or encrypt the Private Key with at least 128 bits of encryption strength. Allowed methods include using a 128-bit AES key to wrap the private key or storing the key in a PKCS 12 file encrypted with a randomly generated password of more than 16 characters containing uppercase letters, lowercase letters, numbers, and symbols for transport.

For Certificates transported outside of a Signing Service's secure infrastructure, the CA or Signing Service MUST require, by contract, each Subscriber to generate their own Private Key and protect the Private Key in accordance with Section 16.2 ("Private Key Protection").

10.3 Subscriber Agreement

10.3.1 General

As specified in BR Section 9.6.3.

Commented [CB37]: 4.1.2

Commented [CB38]: 4.2.1

Commented [CB39]: 6.1.2

Commented [CB40]: This is nonsensical, but has been moved to 6.2.6 anyway

Commented [CB41]: The complete text from BR 9.6.3 was pulled into 9.6.3 as there are CSBR-specific clauses

10.3.2 Agreement Requirements

Commented [CB42]: 9.6.3

The Applicant MUST make the following obligations and warranties through a Subscriber Agreement or Terms of Use:

Commented [CB43]: 9.6.3 already says this

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 16, 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.

10.3.3 Service Agreement Requirements for Signing Services

Commented [CB44]: 9.6.5

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 the Signing Service'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 private 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.

11. Verification Practices

11.1 Verification for Non-EV Code Signing Certificates

Commented [CB45]: 3.2.2.1

11.1.1 Verification of Organizational Applicants

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 BR Sections 3.2.2.1 and 3.2.2.2. 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 BR Section 3.2.2.1,

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 BR 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 11.1.2.

11.1.2 Verification of Individual Applicants

Commented [CB46]: 3.2.3

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.

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

Commented [CB47]: 3.2.3.1

1. The CA MUST obtain a legible copy, which discernibly shows the 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 Requester using (i) a government-issued photo ID, (ii) a QIIS or QGIS, or (iii) an access code to activate the Certificate where the access code was physically mailed to the Requester; OR

2. The CA MUST have the Requester digitally sign the Certificate Request using a valid personal Certificate that was issued under one of the following adopted standards: Qualified Certificates for electronic signatures issued pursuant to Regulation (EU) 2014/910 (eIDAS), 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.

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

Commented [CB48]: 3.2.3.2

1. Having the Requester provide a photo of the 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 Requester where an employee or contractor of the CA can see the Requester, review the Requester's photo ID, and confirm that the Requester is the individual identified in the submitted photo ID; OR

3. Having the CA obtain an executed Declaration of Identity of the 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 Section 11.2.1(2) 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.

11.2 Verification Practices for EV Code Signing Certificates

Commented [CB49]: 3.2.2.2

11.2.1 Verification Requirements – Overview

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 the EV Guidelines 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;

(A) Verify the Applicant's legal existence and identity (as more fully set forth in Section 11.2.3 herein),

(B) Verify the Applicant's physical existence (business presence at a physical address), and

(C) Verify the Applicant's operational existence (business activity).

(2) Verify the Applicant's authorization for the EV Code Signing Certificate, including;

(A) Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,

(B) 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

(C) Verify that a Certificate Approver has signed or otherwise approved the EV Code Signing Certificate Request.

11.2.2 Acceptable Methods of Verification – Overview

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 in the EV Guidelines. 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.

11.2.3 Verification of Applicant's Legal Existence and Identity

As specified in EV Guidelines Section 11.2.

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

As specified in EV Guidelines Section 11.3.

11.2.5 Verification of Applicant's Physical Existence

As specified in EV Guidelines Section 11.4.

11.2.6 Verified Method of Communication

As specified in EV Guidelines Section 11.5.

11.2.7 Verification of Applicant's Operational Existence

As specified in EV Guidelines Section 11.6.

11.2.8 Verification of Applicant's Domain Name

Code Signing Certificates SHALL NOT include a Domain Name.

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

As specified in EV Guidelines Section 11.8.

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

As specified in EV Guidelines Section 11.9.

11.2.11 Verification of Approval of EV Code Signing Certificate Request

As specified in EV Guidelines Section 11.10.

11.2.12 Verification of Certain Information Sources

As specified in EV Guidelines Section 11.11.

11.2.13 Parent/Subsidiary/Affiliate Relationship

As specified in EV Guidelines Section 11.12.3.

11.3 Age of Certificate Data

Commented [CB50]: 4.2.1

For Non-EV Code Signing Certificates, the CA MAY use the documents and data provided in Section 11 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 11 or completed the validation itself no more than 825 days prior to issuing the Certificate.

For EV Code Signing Certificates per EV Guidelines Section 11.14.

Methods 4, 5 and 7 of section 16.3.2 may be reused if Subscriber Private Key protection has been validated no more than 13 months prior to issuing the Code Signing Certificate.

11.4 Denied List

Commented [CB51]: 4.1.1

For Non-EV Code Signing Certificates as specified in BR Section 4.1.1 and for EV Code Signing Certificates as specified in EV Guidelines Section 11.12.2.

11.5 High Risk Certificate Requests

Commented [CB52]: 4.2.1

In addition to the procedures required by BR Section 4.2.1, 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 determine whether the entity is identified as requesting a Code Signing Certificate from a High Risk Region of Concern. 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.

A CA identifying a high risk application under this section MUST follow the additional procedures defined in Section 11.7 of this document to ensure that the applicant will protect its Private Keys and not sign Suspect Code.

[These requirements do not specify a particular database and leave the decision of qualifying databases to the implementers.]

11.6 Data Source Accuracy

Commented [CB53]: 3.2.7

As specified in BR Section 3.2.2.7.

11.7 Processing High Risk Applications

Commented [CB54]: 4.2.2

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 either a loss of control of their code-signing service or loss of the Private Key associated with their Code Signing Certificate.

If the CA is aware that the Applicant was the victim of a Takeover Attack, the CA MUST verify that the Applicant is protecting its Code Signing Private Keys under Section 16.3.1(1) or Section 16.3.1(2). The CA MUST verify the Applicant's compliance with Section 16.3.1(1) or Section 16.3.1(2) (i) through technical means that confirm the Private Keys are protected using the method described in 16.3.1(1) or 16.3.1(2) or (ii) by relying 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.

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

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 either Section 16.3.1 (1) or 16.3.1 (2).

11.8 Due Diligence

Commented [CB55]: 4.2.1

As specified in Section 11.13 of the EV Guidelines.

12. Certificate Issuance by a Root CA

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.

Commented [CB56]: 4.3.1

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

Commented [CB57]: 6.1.7

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.

13. Certificate Revocation and Status Checking

13.1 Revocation

13.1.1 Revocation Request

Commented [CB58]: 4.9.3

As specified in BR Section 4.9.3.

13.1.2 Certificate Problem Reporting

Commented [CB59]: 4.9.2

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.

13.1.3 Investigation

Commented [CB60]: 4.9.3

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.

13.1.4 Response

Commented [CB61]: 4.9.3

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.

13.1.5 Reasons for Revoking a Subscriber Certificate

Commented [CB62]: 4.9.1

A CA MUST revoke a Code Signing Certificate in any of the four circumstances: (1) the Application Software Supplier requests revocation, (2) the subscriber requests revocation, (3) a third party provides information that leads the CA to believe that the certificate is compromised or is being used for Suspect Code, or (4) the CA otherwise decides that the certificate should be revoked. This section describes the CA's obligations for each scenario.

13.1.5.1 Revocation Based on an Application Software Supplier's Request

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

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

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

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

13.1.5.2 Revocation Based on the Subscriber's Request

The CA MUST revoke a Code Signing Certificate within one (1) business day if the Subscriber requests in writing that the CA revoke the Certificate or notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization.

13.1.5.3 Revocation Based on Reported or Detected Compromise or Use in Malware

For all incidents involving malware, CAs SHALL revoke the Code Signing Certificate in accordance with and within the following maximum timeframes. Nothing herein prohibits a CA from revoking a Code Signing Certificate prior to these timeframes.

1. The CA MUST contact the software publisher within one (1) business day after the CA is made aware of the incident.
2. The CA MUST determine the volume of relying parties that are impacted (e.g., based on OCSP logs) within 72 hours after being made aware of the incident.
3. The CA MUST request the software publisher send an acknowledgement to the CA within 72 hours of receipt of the request.
    a. If the publisher responds within 72 hours, the CA and publisher MUST determine a "reasonable date" to revoke the certificate based on discussions with the CA.
    b. If CA does not receive a response, the CA must notify the publisher that the CA will revoke in 7 days if no further response is received.
        i. If the publisher responds within 7 days, the CA and the publisher will determine a "reasonable date" to revoke the certificate based on discussion with the CA.
        ii. If no response is received after 7 days, the CA must revoke the certificate except if the CA has documented proof (e.g., OCSP logs) that the revocation will cause significant impact to the general public.

A CA revoking a Certificate because the Certificate was associated with signed Suspect Code or other fraudulent or illegal conduct SHOULD provide all relevant information and risk indicators to other CAs or industry groups. The CA SHOULD indicate whether its investigation found that the Suspect Code was a false positive or an inadvertent signing.

13.1.6 Reasons for Revoking a Subordinate CA Certificate

Commented [CB63]: 4.9.1.4

As specified in BR Section 4.9.1.2.

13.1.7 Certificate Revocation Date

Commented [CB64]: 4.9.5

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.

13.2 Certificate Status Checking

13.2.1 Mechanisms

In addition to the requirements specified in BR Section 4.9.7 through 4.9.10 (BR Section 4.9.9 and 4.9.10 are only required if the CA provides OCSP responses), CAs MUST provide up-to-date revocation status information. CAs MUST issue CRLs, and the serial number of a revoked certificate MUST remain on the CRL for at least 10 years after the expiration of the certificate. 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. Application Software Suppliers MAY require the CA to support a longer life-time in its contract with the CA. 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.

Commented [CB65]: This was further fleshed out in 4.9.7

Commented [CB66]: 7.2

Commented [CB67]: 4.9.10

Commented [CB68]: 7.2

Commented [CB69]: 5.8

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.

Commented [CB70]: 7.2

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.

Commented [CB71]: 4.9.6

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.

Commented [CB72]: 4.9.11

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 and OCSP responses for that Code Signing Certificate.

Commented [CB73]: Duplicated to 7.2 and 7.3

---

[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.

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.

Commented [CB74]: 7.2.2

13.2.2 Repository

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.

Commented [CB75]: 4.9.9

For the status of Subordinate CA Certificates:

Commented [CB76]: 4,9,7

1. 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; and

2. 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:

1. 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; and

2. If the Subordinate CA provides OCSP responses, the Subordinate 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:

1. The Subordinate CA SHALL update and reissue CRLs at least (i) once every twelve months and (ii) 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; and

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

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

Commented [CB77]: 4,9,10

14. Employees and Third Parties

14.1 Trustworthiness and Competence

For Non-EV Code Signing Certificates as specified in BR Section 5.3 and for EV Code Signing Certificates as specified in EV Guidelines Section 14.1.

After 2021-06-01, the CA shall meet the requirements of EV Guidelines Section 14.1 for Non-EV and EV Code Signing Certificates.

14.2 Delegation of Functions to Registration Authorities and Subcontractors

14.2.1 General

Except as stated in Section 14.2.2 of this document, 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 BR Section 5.3 when applicable to the delegated function,
2. Retain documentation in accordance with BR 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 the Signing Service and any other Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 of this document and the document retention and event logging requirements of Section 15 of this document.

If a Delegated Third Party fulfills any of the CA's obligations under Section 11.5 (High Risk Requests) of this document, the CA MUST verify that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as the CA's own processes.

14.2.2 Compliance Obligation

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.

14.2.3 Allocation of Liability

As specified in Section BR Sections 9.8 and 9.9.

Commented [CB78]: 5,3

Commented [CB79]: This was simplified as the transition date has already passed

Commented [CB80]: 8 (5)

Commented [CB81]: 1.3.2

Commented [CB82]: 1.3.2

Commented [CB83]: 9.8 and 9.9. This text was modified in these two sections to align the BRs and CSBRs.

15. Data Records

15.1 Types of Events Recorded

Commented [CB84]: 5.4.1.1

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

Log entries MUST include the following elements:

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

15.2 Timestamp Authority Data Records

Commented [CB85]: 5.4.1.2

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:

   a. Successful and unsuccessful Timestamp Authority access attempts;

   b. Timestamp Authority server actions performed;

   c. Security profile changes;

   d. System crashes and other anomalies; and

   e. Firewall and router activities;

5. f. Revocation of a timestamp certificate,

6. Major changes to the timestamp server's time, and

7. System startup and shutdown.

15.3 Data Retention Period for Audit Logs

Commented [CB86]: 5.4.3

The CA, Delegated Third Parties, and Timestamp Authority MUST retain, for at least two years:

1. CA certificate and key lifecycle management event records (as set forth in Section 15.1 (1)) after the later occurrence of:
   a. the destruction of the CA Private Key; or
   b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 15.1 (2)) after the revocation or expiration of the Subscriber Certificate;
3. Timestamp Authority data records (as set forth in Section 15.2) after the revocation or renewal of the Timestamp Certificate private key (as set forth in Section 9.4);
4. Any security event records (as set forth in Section 15.1 (3) and for Timestamp Authority security event records set forth in Section 15.2(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.

16. Data Security and Private Key Protection

The requirements in BR Sections 5, 6.1 and 6.2 apply equally to Code Signing Certificates.

Commented [CB87]: 6.2.7.4

16.1 Timestamp Authority Key Protection

1. 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 a Timestamp Authority to timestamp signed code.

Commented [CB88]: 6.8

2. A Timestamp Authority MUST protect its signing key using a process that is at least to FIPS 140-2 Level 3, Common Criteria EAL 4+ (ALC_FLR.2), or higher. The CA MUST protect its signing operations in accordance with the CA/Browser Forum's Network Security Guidelines. Any changes to its signing process MUST be an auditable event.

Commented [CB89]: 6.2.7.2

Commented [CB90]: 6.8

3. 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.

Commented [CB91]: 6.8

16.2 Signing Service Requirements

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 to access and authorize Code Signing and obtain a representation from the Subscriber that they will securely store the tokens required for multi-factor access. A system used to host a Signing Service MUST NOT be used for web browsing. The Signing Service MUST run a regularly updated antivirus solution to scan the service for possible virus infection. The Signing Service MUST comply with the Network Security Guidelines as a "Delegated Third Party".

Commented [CB92]: 6.2.7.3

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

Techniques that MAY be used to satisfy this requirement include:

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

4. Contractual terms in the subscriber agreement requiring the Subscriber to protect the Private Key to a standard of at least FIPS 140-2 level 2 or Common Criteria EAL 4+ and with compliance being confirmed by means of an audit.

Cryptographic algorithms, key sizes and certificate life-times for both authorities and Subscribers are governed by the NIST key management guidelines.

Commented [CB93]: 6.3.2

16.3 Subscriber Private Key Protection and Verification

Commented [CB94]: 6.2.7.4

16.3.1 Subscriber Private Key Protection

For Non-EV Code Signing Certificates issued prior to November 15, 2022, 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 November 15, 2022, a CA MUST recommend that the Subscriber protect Private Keys using the method described in Section 16.3.1(1) or 16.3.1(2) over the method described in Section 16.3.1(3) and obligate the Subscriber to protect Private Keys in accordance with 10.3.2(2)

For EV Code Signing Certificates issued prior to November 15, 2022, 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.

Commented [IM95]: From Tim H: There a fair amount of concern that this language can be abused to allow things that aren't actually key attestation, but we're struggling to find language to fix it in the absence of good key attestation standards to point to (anyone know of one?). Perhaps just adding something like ("commonly known as key attestation") will be a hint to auditors and CAs that that's what we want here.

Commented [IM96R95]: I like adding the hint you provided here, so let's add it to the new requirements as this reference will be removed post 11/15/2022.

Effective November, 15, 2022, 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:

   a Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements;

   b Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.

9. Subscriber uses a Signing Service which meets the requirements of section 16.2.

16.3.2 Subscriber Private Key Verification

Effective November, 15, 2022, 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 16.3.1. 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;

Commented [IM97]: From Tim H: There a fair amount of concern that this language can be abused to allow things that aren't actually key attestation, but we're struggling to find language to fix it in the absence of good key attestation standards to point to (anyone know of one?). Perhaps just adding something like ("commonly known as key attestation") will be a hint to auditors and CAs that that's what we want here.

Commented [IM98R97]: I like the idea of adding the "hint" text you provided, so I've added here.

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 16.2;

8. Any other method the CA uses to satisfy this requirement. 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 November 15, 2022, 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.

Commented [IM99]: From Tim H: This doesn't English.

Commented [IM100R99]: Yeah, it definitely doesn't English. ☹
I think we are saying a CA is relying on a report...

17. Audit

17.1 Eligible Audit Schemes

Commented [CB101]: 8.4

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

1. For Audit Periods starting before 1 November 2020, "WebTrust for CAs v2.0 or newer" AND "WebTrust for Certification Authorities – Publicly Trusted Code Signing Certificates v1.0.1 or newer"; or

2. For Audit Periods starting before 1 November 2020, "WebTrust for CAs v2.0 or newer" AND "WebTrust for Certification Authorities – Extended Validation Code Signing v1.4.1 or newer"; or

3. "WebTrust for CAs v2.0 or newer" AND "WebTrust for Certification Authorities – Code Signing Baseline Requirements v2.0 or newer"; or

4. 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

5. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either (a) encompasses all requirements of one of the above schemes or (b) consists of comparable criteria that are available for public review.

Whichever scheme is chosen, it 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.

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

17.2 Audit Period

Commented [CB102]: 8.1

As specified in BR Section 8.1.

Commented [CB103]: Text from BR 8.1 was pulled directly in as there was CSBR-specific content

17.3 Audit Report

Commented [CB104]: 8.6

As specified in BR Section 8.6.

17.4 Pre-Issuance Readiness Audit

Commented [CB105]: 8.1

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 17.1, 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 17.1, 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 17.1. 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.

17.5 Regular Self Audits

Commented [CB106]: 8.7

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.

17.6 Audit of Delegated Functions

Commented [CB107]: 8.1

Audits MUST be conducted for all obligations under these Guidelines, including timestamping and signing services, regardless of whether they are performed directly by the CA or by a Delegated Third Party. 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).

17.7 Auditor Qualifications

Commented [CB108]: 8.2

As specified in BR Section 8.2.

17.8 Key Generation Ceremony

Commented [CB109]: 6.1.1.1

As specified in BR Section 6.1.1.1.

18. Liability and Indemnification

CAs MAY limit their liability as described in Section 9.8 of the Baseline Requirements except for EV Code Signing Certificates, a CA MAY 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.

Commented [CB110]: 9.8

A CA's indemnification obligations and a Root CA's obligations with respect to subordinate CAs are set forth in Section 9.9 of the Baseline Requirements

Commented [CB111]: 9.9

Appendix A

Minimum Cryptographic Algorithm and Key Size Requirements

Certificates and Timestamp tokens issued after 31 January 2017 MUST meet the following requirements for algorithm type and key size.

(1) Code Signing Root, Subordinate CA, and Code Signing Certificates

The table below defines cryptographic requirements for Code Signing Certificates issued within the specified time and their corresponding Root Certificates and Subordinate CA Certificates.

Note: The digest algorithm used to issue the Root Certificate does not have security relevance and need not conform to the requirements in the table below.

	Code Signing Certificates issued prior to the transition date and their corresponding Root Certificates and Subordinate CA Certificates	Transition date	Code Signing Certificates issued on or after the transition date and their corresponding Root Certificates and Subordinate CA Certificates
Digest algorithm	SHA-256, SHA-384 or SHA-512 (SHA-1 for legacy implementations only)*	January 1, 2021	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048	June 1, 2021	**4096 for Root and Subordinate CA Certificates 3072 for Code Signing Certificates
ECC curve	NIST P-256, P-384, or P-521		NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048, N= 224 or L= 2048, N= 256		L= 2048, N= 224 or L= 2048, N= 256

*CAs can issue SHA-1 certificates to legacy platforms that do not support SHA-2 only for code signing and timestamping certificates.

Commented [CB112]: This has been split between sections 6.1.5 and 7.1.3

Commented [CB113]: This is addressed in 7.1.3.2, albeit with no "legacy platform" wording

**CAs can issue Cross Certificates for Root CAs whose Public Key meets the above requirements in force after the Transition Date with a Root whose Public Key meets the above requirements in force prior to the Transition Date to support Code Signing Certificate validation.

Commented [CB114]: 6.1.5

(2) Timestamp Root, Subordinate CA, and Timestamp Certificates

The table below defines cryptographic requirements for Timestamp Certificates issued within the specified time and their corresponding Root Certificates and Subordinate CA Certificates.

Note: The digest algorithm used to issue the Root Certificate does not have security relevance and need not conform to the requirements in the table below.

	Timestamp Certificates issued prior to the transition date and their corresponding Root Certificates and Subordinate CA Certificates	Transition Date	Timestamp Certificates issued on or after the transition date and their corresponding Root Certificates and Subordinate CA Certificates
Digest algorithm	SHA-256, SHA-384 or SHA-512 (SHA-1 for legacy implementations only)*	April 30, 2022	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048	June 1, 2021	**4096 for Root and Subordinate CA Certificates 3072 for TimestampCertificates
ECC curve	NIST P-256, P-384, or P-521		NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048, N= 224 or L= 2048, N= 256		L= 2048, N= 224 or L= 2048, N= 256

*CAs can issue SHA-1 certificates to legacy platforms that do not support SHA-2 only for code signing and timestamping certificates.

**CAs can issue Cross Certificates for Root CAs whose Public Key meets the above requirements in force after the Transition Date with a Root whose Public Key meets the above requirements in force prior to the Transition Date to support Timestamp Certificate validation.

Commented [CB115]: 6.1.5

(3) Timestamp Tokens

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

	Generated prior to transition date	Transition date	Generated on or after transition date
Digest algorithm	SHA-256, SHA-384 or SHA-512 (SHA-1 for legacy implementations only)*	April 30, 2022	SHA-256, SHA-384 or SHA-512

*CAs can issue SHA-1 certificates to legacy platforms that do not support SHA-2 only for code signing and timestamping certificates no later than April 30, 2022.

Commented [CB116]: 6.8

Commented [CB117]: This table has been migrated to text in 7.1.3.2

Commented [CB118]: This is addressed in 7.1.3.2, albeit with no "legacy platform" wording

Appendix B

Certificate Extensions (Normative)

This appendix specifies the requirements for extensions in Certificates issued after the date of these guidelines (including Subordinate CA certificates)

(1) Root CA Certificates

As specified in Section 7.1.2.1 of the Baseline Requirements.

(2) Certificates for Subordinate CAs issuing Code Signing Certificates

A. certificatePolicies

Refer to certificate policy identification requirements in Section 9.3.3.

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

certificatePolicies:policyIdentifier (Required)

If the certificate is issued to a Subordinate CA that is not an Affiliate of the entity that controls the Root CA, then the set of policy identifiers MUST include a Policy Identifier, defined by the Subordinate CA, which indicates a Certificate Policy asserting the Subordinate CA's adherence to and compliance with these Requirements.

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

- id-qt 1 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier:cPSuri

- HTTP URL for the Root CA's Certification Practice Statement

B. cRLDistributionPoint

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

C. authorityInformationAccess

This extension MUST be present and MUST NOT be marked critical. The extension MUST contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and if the CA provides OCSP responses, the HTTP URL for the CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

Commented [CB119]: 7.1.2.1

Commented [CB120]: Requirements in BR have been pulled in directly to merge CSBR-specific requirements

Commented [CB121]: 7.1.2.2; with the exception of EKU, the extension requirements are the same for CS and TS ICAs, so they have been merged

Commented [CB122]: 7.1.6.3

D. basicConstraints

This extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. 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 (EKU)

The id-kp-codeSigning [RFC5280] value MUST be present.

.

The following EKUs MUST NOT be present: anyExtendedKeyUsage (2.5.29.37.0), serverAuth (1.3.6.1.5.5.7.3.1), emailProtection (1.3.6.1.5.5.7.3.4) and timeStamping (1.3.6.1.5.5.7.3.8).

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.

This extension SHOULD be marked non-critical.

The CA MUST set all other fields and extensions in accordance to RFC 5280.

Commented [CB123]: Pulled in BR 7.1.2.4 to address this.

(3) Code Signing Certificates

Commented [CB124]: 7.1.2.3; CS and TS end-entity certificate profiles are identical except EKU so they have been merged

A. certificatePolicies

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

certificatePolicies:policyIdentifier (Required)

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

certificatePolicies:policyQualifiers:policyQualifierId (Recommended)

- id-qt 1 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

- HTTP URL for the Subordinate CA's Certification Practice Statement

B. cRLDistributionPoint

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 and MUST NOT be marked critical. The extension MUST contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and if the CA provides OCSP responses, the HTTP URL for the CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

D. basicConstraints (optional)

If present, the cA field MUST be set false.

E. keyUsage (required)

This extension MUST be present and MUST be marked critical. The bit positions 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 (EKU) (required)

The value id-kp-codeSigning [RFC5280] MUST be present.

The following EKUs MAY be present: documentSigning, lifetimeSigning, and emailProtection.

The value anyExtendedKeyUsage (2.5.29.37.0) or serverAuth (1.3.6.1.5.5.7.3.1) MUST NOT be present.

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.

The CA MUST set all other fields and extensions in accordance to RFC 5280.

Commented [CB125]: 7.1.2.4

(4) Certificates for Subordinate CAs issuing Timestamp Certificates

Commented [CB126]: Merged with CS ICA requirements in 7.1.2.2

A. certificatePolicies

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

certificatePolicies:policyIdentifier (Required)

If the certificate is issued to a Subordinate CA that is not an Affiliate of the entity that controls the Root CA, then the set of policy identifiers MUST include a Policy Identifier, defined by the Subordinate CA, which indicates a Certificate Policy asserting the Subordinate CA's adherence to and compliance with these Requirements.

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

- id-qt 1 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier:cPSuri

- HTTP URL for the Root CA's Certification Practice Statement

B. cRLDistributionPoint

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

C. authorityInformationAccess

This extension MUST be present and MUST NOT be marked critical. The extension MUST contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and if the CA provides OCSP responses, the HTTP URL for the CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

D. basicConstraints

This extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. 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 (EKU)

The id-kp-timeStamping [RFC5280] value MUST be present.

The value anyExtendedKeyUsage (2.5.29.37.0) MUST NOT be present.

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.

This extension SHOULD be marked non-critical.

The CA MUST set all other fields and extensions in accordance to RFC 5280.

(5) Timestamp Certificates

Commented [CB127]: Merged with CS end-entity profile in 7.1.2.3. Only difference is EKU and its criticality

A. certificatePolicies

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

certificatePolicies:policyIdentifier (Required)

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

certificatePolicies:policyQualifiers:policyQualifierId (Recommended)

- id-qt 1 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

- HTTP URL for the Subordinate CA's Certification Practice Statement

B. cRLDistributionPoint

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 and MUST NOT be marked critical. The extension MUST contain the HTTP URL for the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and if the CA provides OCSP responses, the HTTP URL of the CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

D. basicConstraints (optional)

If present, the cA field MUST be set false.

E. keyUsage (required)

This extension MUST be present and MUST be marked critical. The bit positions 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 (EKU) (required)

The value id-kp-timeStamping [RFC5280] MUST be present and MUST be marked critical.

The value anyExtendedKeyUsage (2.5.29.37.0) MUST NOT be present.

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.

The CA MUST set all other fields and extensions in accordance to RFC 5280.

Appendix C

Commented [CB128]: 3.2.6

User Agent Interoperability Verification (Normative)

The CA SHOULD issue Code Signing and Timestamping 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 Timestamping Certificates that are valid (non-revoked and unexpired).

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 11.7 of this document:

NONE