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

Version 3.1~~0~~.0

CA/Browser Forum

~~XX XXXX~~September 19, 2022

Table of Contents

1. INTRODUCTION

1.1 Overview

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

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

1.2 Document name and identification

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

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

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

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

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

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

1.2.1 Revisions

Ver.	Ballot	Description	Effective
1.2	CSC-1	Adopt Baseline Requirements version 1.2	13 Aug 2019
2.0	CSC-2	Adopt combined EV and BR Code Signing Document	2 Sept 2020
2.1	CSC-4	Move deadline for transition to RSA-3072 and SHA-2 timestamp tokens	7 Nov 2020
2.2	CSC-7	Update to merge EV and non-EV clauses	8 March 2021
2.3	CSC-8	Update to Revocation response mechanisms. key protection for EV certificates, and clean-up of 11.2.1 & Appendix B	2 May 2021
2.4	CSC-9	Spring 2021 Clean-up and Clarification	8 September 2021
2.5	CSC-10	WebTrust CSBR v2.0 Audit Criteria	12 September 2021
2.6	CSC-11	Update to log data retention requirements	3 November 2021
2.7	CSC-12	CRL Revocation Date Clarification	3 December 2021
2.8	CSC-13	Update to Subscriber Key Protection Requirements	6 May 2022

1.2.2 Relevant Dates

Compliance	Section(s)	Summary Description (See Full Text for Details)
2021-06-01	6.1.5	CAs SHALL support minimum RSA-3072 for Code Signing Certificates, Root Certificates and Subordinate CA Certificates. CAs SHALL NOT support SHA-1 digest algorithm for Code Signing Certificates.
2021-06-01	5.3	After 2021-06-01, the CA shall meet the requirements of EV

		Guidelines Section 14.1 for Non-EV and EV Code Signing Certificates.
2021-06-01	6.2.7.4	For EV Code Signing Certificates, Signing Services shall protect private keys in a FIPS 140-2 level 2 (or equivalent) crypto module. After 2021-06-01, the same protection requirements SHALL apply to Non EV Code Signing Certificates.
2021-11-01	3.2.2.1 (5)	The method used to verify the identity of the Certificate Requester SHALL be per section 3.2.3.
2022-03-31	7.1.6.3	Subordinate CA Certificates issued for Subordinate CA that issues Timestamp Certificates and is an Affiliate of the Issuing CA must include the reserved identifier specified in Section 7.1.6.1.
2022-04-30	7.1.3.2.1	CAs SHALL NOT support SHA-1 digest algorithm for Timestamp tokens.
2022-07-01	7.2.2	For Code Signing Certificates, the time encoded in the Invalidity Date CRL entry extension MUST be equal to the time encoded in the revocationDate field of the CRL entry.
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.

1.3 PKI participants

1.3.1 Certification authorities

1.3.2 Registration authorities

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

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

1. Meet the qualification requirements of 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 5.3 of this document and the document retention and event logging requirements of Section 5.4 of this document.

If a Delegated Third Party fulfills any of the CA's obligations under Section 4.2.1 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.

1.3.3 Subscribers

1.3.4 Relying parties

1.3.5 Other participants

1.4 Certificate usage

1.4.1 Appropriate certificate uses

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

1.4.2 Prohibited certificate uses

1.5 Policy administration

1.5.1 Organization administering the document

1.5.2 Contact person

1.5.3 Person determining CPS suitability for the policy

1.5.4 CPS approval procedures

1.6 Definitions and acronyms

1.6.1 Definitions

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

Certificate 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.

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 A, a geographic location where the detected number of Code Signing Certificates associated with signed Suspect Code exceeds 5% of the total number of detected Code Signing Certificates originating or associated with the same geographic area.

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.

1.6.2 Abbreviations and Acronyms

As specified in the Baseline Requirements and EV Guidelines.

1.6.3 References

This document references the following CA/B Forum documents: * The Baseline Requirements, version 1.6.9 * The EV Guidelines, version 1.7.2

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

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

1.6.4 Conventions

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

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

2.2 Publication of certification information

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

Each CA MUST represent that it has disclosed all Cross Certificates in its Certificate Policy/Certificate Practice Statement that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

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

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

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

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

2.3 Time or frequency of publication

2.4 Access controls on repositories

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

3.1.2 Need for names to be meaningful

3.1.3 Anonymity or pseudonymity of subscribers

3.1.4 Rules for interpreting various name forms

3.1.5 Uniqueness of names

3.1.6 Recognition, authentication, and role of trademarks

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

3.2.2 Authentication of organization identity

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

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

1. Verify the Subject's legal identity, including any DBA proposed for inclusion in a Certificate, in accordance with 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 3.2.3.1.

3.2.2.2 Authentication of organization identity for EV Code Signing Certificates

Before issuing a EV Code Signing Certificate, the CA MUST ensure that all Subject organization information to be included in the EV Code Signing Certificate conforms to the requirements of, and is verified in accordance with 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 3.2.2.2.1 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.

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.

Roles are specified in EV Guidelines Section 10.1.2.

3.2.2.2.1 Verification of Applicant's Legal Existence and Identity

As specified in EV Guidelines Section 11.2.

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

As specified in EV Guidelines Section 11.3.

3.2.2.2.3 Verification of Applicant's Physical Existence

As specified in EV Guidelines Section 11.4.

3.2.2.2.4 Verified Method of Communication

As specified in EV Guidelines Section 11.5.

3.2.2.2.5 Verification of Applicant's Operational Existence

As specified in EV Guidelines Section 11.6.

3.2.2.2.6 Verification of Applicant's Domain Name

Code Signing Certificates SHALL NOT include a Domain Name.

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

As specified in EV Guidelines Section 11.8.

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

As specified in EV Guidelines Section 11.9.

3.2.2.2.9 Verification of Approval of EV Code Signing Certificate Request

As specified in EV Guidelines Section 11.10.

3.2.2.2.10 Verification of Certain Information Sources

As specified in EV Guidelines Section 11.11.

3.2.2.2.11 Parent/Subsidiary/Affiliate Relationship

As specified in EV Guidelines Section 11.12.3.

3.2.3 Authentication of individual identity

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

3.2.3.1 Individual identity verification

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

1. The CA MUST obtain a legible copy, which discernibly shows the 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 issued pursuant to ETSI TS 101 862, IGTF, Adobe Signing Certificate issued under the AATL or CDS program, the Kantara identity assurance

framework at level 2, NIST SP 800-63 at level 2, or the FBCA CP at Basic or higher assurance.

3.2.3.2 Authenticity of Certificate requests for Individual Applicants

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

1. Having the 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 item (2) of Section 3.2.3.1 is a valid signature and originated from a Certificate issued at the appropriate level of assurance as evidenced by the certificate chain. Acceptable verification under this section includes validation that the Certificate was issued by a CA qualified by the entity responsible for adopting, enforcing, or maintaining the adopted standard and chains to an intermediate certificate or root certificate designated as complying with such standard.

3.2.4 Non-verified subscriber information

3.2.5 Validation of authority

3.2.6 Criteria for interoperation

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

3.2.7 Data source accuracy

As specified in BR Section 3.2.2.7.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

3.3.2 Identification and authentication for re-key after revocation

3.4 Identification and authentication for revocation request

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

For Non-EV Code Signing Certificates, the CA SHALL implement procedures to identify suspicious certificate requests as defined in BR Section 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. The CA SHALL implement procedures to identify suspicious certificate requests as defined in EV Guidelines Section 11.12.2.

4.1.2 Enrollment process and responsibilities

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

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.

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.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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.

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 4.2.2 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.]

Prior to issuing Code Signing Certificates, the CA SHALL perform “due diligence” verification as specified in EV Guidelines 11.13.

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

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

For EV Code Signing Certificates, use of documents, data, and previous validations performed per Section 3.2 SHALL be governed by the usage periods as defined in EV Guidelines Section 11.14.

4.2.2 Approval or rejection of certificate applications

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

Certificate was not revoked because the Applicant was intentionally signing Suspect Code.

CAs MAY issue new or replacement Code Signing Certificates to an entity who is the victim of a documented Takeover Attack, resulting in 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 6.2.7.4.1(1) or Section 6.2.7.4.1(2). The CA MUST verify the Applicant's compliance with Section 6.2.7.4.1(1) or Section 6.2.7.4.1(2) through: 1. Technical means that confirm the Private Keys are protected using the method described in Section 6.2.7.4.1(1) or Section 6.2.7.4.1(2); or 2. 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 Section 6.2.7.4.1(1) or Section 6.2.7.4.1(2).

4.2.3 Time to process certificate applications

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

4.3.2 Notification to subscriber by the CA of issuance of certificate

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

4.4.2 Publication of the certificate by the CA

4.4.3 Notification of certificate issuance by the CA to other entities

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

4.5.2 Relying party public key and certificate usage

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

4.6.2 Who may request renewal

4.6.3 Processing certificate renewal requests

4.6.4 Notification of new certificate issuance to subscriber

4.6.5 Conduct constituting acceptance of a renewal certificate

4.6.6 Publication of the renewal certificate by the CA

4.6.7 Notification of certificate issuance by the CA to other entities

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

4.7.2 Who may request certification of a new public key

4.7.3 Processing certificate re-keying requests

4.7.4 Notification of new certificate issuance to subscriber

4.7.5 Conduct constituting acceptance of a re-keyed certificate

4.7.6 Publication of the re-keyed certificate by the CA

4.7.7 Notification of certificate issuance by the CA to other entities

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

4.8.2 Who may request certificate modification

4.8.3 Processing certificate modification requests

4.8.4 Notification of new certificate issuance to subscriber

4.8.5 Conduct constituting acceptance of modified certificate

4.8.6 Publication of the modified certificate by the CA

4.8.7 Notification of certificate issuance by the CA to other entities

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

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.

4.9.1.1 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.

4.9.1.2 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.

4.9.1.3 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.

4.9.1.4 Revocation of a Subordinate CA Certificate

As specified in BR Section 4.9.1.2.

4.9.2 Who can request revocation

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

4.9.3 Procedure for revocation request

As specified in BR Section 4.9.3.

4.9.4 Revocation request grace period

4.9.5 Time within which CA must process the revocation request

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

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

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

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

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

4.9.6 Revocation checking requirement for relying parties

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

4.9.7 CRL issuance frequency

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

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

For the status of Timestamp Certificates: * The Subordinate CA SHALL update and reissue CRLs at least once every twelve months and within 24 hours after revoking a Timestamp Certificate, and the value of the `nextUpdate` field MUST NOT be more than twelve months beyond the value of the `thisUpdate` field.

4.9.8 Maximum latency for CRLs

4.9.9 On-line revocation/status checking availability

4.9.10 On-line revocation checking requirements

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

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

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

For the status of Code Signing Certificates: * If the Subordinate CA provides OCSP responses, the CA SHALL update information provided via an OCSP response at least

[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.

every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.

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

4.9.11 Other forms of revocation advertisements available

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

4.9.12 Special requirements re key compromise

4.9.13 Circumstances for suspension

4.9.14 Who can request suspension

4.9.15 Procedure for suspension request

4.9.16 Limits on suspension period

4.10 Certificate status services

4.10.1 Operational characteristics

4.10.2 Service availability

4.10.3 Optional features

4.11 End of subscription

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

4.12.2 Session key encapsulation and recovery policy and practices

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

5.1.2 Physical access

5.1.3 Power and air conditioning

5.1.4 Water exposures

5.1.5 Fire prevention and protection

5.1.6 Media storage

5.1.7 Waste disposal

5.1.8 Off-site backup

5.2 Procedural controls

5.2.1 Trusted roles

5.2.2 Number of persons required per task

5.2.3 Identification and authentication for each role

5.2.4 Roles requiring separation of duties

5.3 Personnel controls

As specified in EV Guidelines Section 14.1. Additionally, the CA SHALL require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in these Requirements.

5.3.1 Qualifications, experience, and clearance requirements

5.3.2 Background check procedures

5.3.3 Training requirements

5.3.4 Retraining frequency and requirements

5.3.5 Job rotation frequency and sequence

5.3.6 Sanctions for unauthorized actions

5.3.7 Independent contractor requirements

5.3.8 Documentation supplied to personnel

5.4 Audit logging procedures

5.4.1 Types of events recorded

5.4.1.1 Types of events recorded for CAs

The CA and each Delegated Third Party SHALL record details of the actions taken to process a certificate request and to issue a certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. The CA SHALL make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

The CA SHALL record at least the following events:

1. CA certificate and key lifecycle management events, including: 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.

5.4.1.2 Types of events recorded for Timestamp Authorities

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

1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
2. History of the timestamp server configuration,
3. Any attempt to delete or modify timestamp logs,
4. Security events, including: 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. Revocation of a timestamp certificate,
6. Major changes to the timestamp server's time, and
7. System startup and shutdown.

5.4.2 Frequency of processing log

5.4.3 Retention period for audit log

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

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1.1)(1) after the later occurrence of:

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 5.4.1.2)(2) after the revocation or expiration of the Subscriber Certificate;
3. Timestamp Authority data records (as set forth in Section 5.4.1.2) after the revocation or renewal of the Timestamp Certificate private key (as set forth in Section 6.3.2);
4. Any security event records (as set forth in Section 5.4.1.1(3) and for Timestamp Authority security event records set forth in Section 5.4.1.2(3)) after the event occurred

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

5.4.4 Protection of audit log

5.4.5 Audit log backup procedures

5.4.6 Audit collection system (internal vs. external)

5.4.7 Notification to event-causing subject

5.4.8 Vulnerability assessments

5.5 Records archival

5.5.1 Types of records archived

5.5.2 Retention period for archive

5.5.3 Protection of archive

5.5.4 Archive backup procedures

5.5.5 Requirements for time-stamping of records

5.5.6 Archive collection system (internal or external)

5.5.7 Procedures to obtain and verify archive information

5.6 Key changeover

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

5.7.3 Entity private key compromise procedures

5.7.4 Business continuity capabilities after a disaster

5.8 CA or RA termination

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

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

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA Key Pair Generation

As specified in BR Section 6.1.1.1.

6.1.1.2 RA Key Pair Generation

6.1.1.3 Subscriber Key Pair Generation

The CA SHALL reject a certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 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).

6.1.2 Private key delivery to subscriber

If the CA or any Delegated Third Party is generating the Private Key on behalf of the Subscriber where the Private Keys will be transported to the Subscriber outside of the Signing Service's secure infrastructure, then the entity generating the Private Key MUST 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.

6.1.3 Public key delivery to certificate issuer

6.1.4 CA public key delivery to relying parties

6.1.5 Key sizes

6.1.5.1 Root and Subordinate CA key sizes

For Keys corresponding to Root and Subordinate CAs:

- If the Key is RSA, then the modulus MUST be at least 4096 bits in length. [2]

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

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

6.1.5.2 Code signing Certificate and Timestamp Authority key sizes

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

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

6.1.6 Public key parameters generation and quality checking

6.1.7 Key usage purposes

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

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates);
4. Certificates for OCSP Response verification; and
5. Signatures for OCSP Responses.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

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

6.2.3 Private key escrow

6.2.4 Private key backup

6.2.5 Private key archival

6.2.6 Private key transfer into or from a cryptographic module

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 6.2.7.4.

6.2.7 Private key storage on cryptographic module

6.2.7.1 Private key storage for CA keys

Private Keys corresponding to CA Keys MUST be stored in accordance with BR Section 6.2.7.

6.2.7.2 Private key storage for Timestamp Authorities

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.

6.2.7.3 Private key storage for Signing Services

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

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~~ Hardware ~~crypto~~ Crypto ~~module~~ 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.

6.2.7.4 Subscriber Private Key protection and verification

The requirements in BR Section 6.2 apply equally to Code Signing Certificates.

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

For EV Code Signing Certificates issued prior to 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.

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 6.2.7.3.

6.2.7.4.2 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 6.2.7.4.1. One of the following methods MUST be employed to satisfy this requirement:
1. The CA ships a suitable Hardware Crypto Module, with one or more pre-generated Key Pairs that the CA has generated using the Hardware Crypto Module;

-2. The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate, commonly known as key attestation, indicating that the Private Key was generated in a non-exportable way using a suitable Hardware Crypto Module;

-3. The Subscriber uses a CA prescribed crypto library and a suitable Hardware Crypto Module combination for the Key Pair generation and storage;

4. The Subscriber provides an internal or external IT audit indicating that it is only using a suitable Hardware Crypto Module to generate Key Pairs to be associated with Code Signing Certificates;

5. The Subscriber provides a suitable report from the cloud-based key protection solution subscription and resources configuration protecting the Private Key in a suitable Hardware Crypto Module;

6. The CA relies on a report provided by the Applicant that is signed by an auditor who is approved by the CA and who has IT and security training or is a CISA witnesses the Key Pair creation in a suitable Hardware Crypto Module solution including a cloud-based key generation and protection solution;

7. The Subscriber provides an agreement that they use a Signing Service meeting the requirements of Section 6.2.7.3;

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.

6.2.8 Method of activating private key

6.2.9 Method of deactivating private key

6.2.10 Method of destroying private key

6.2.11 Cryptographic Module Rating

6.3 Other aspects of key pair management

6.3.1 Public key archival

6.3.2 Certificate operational periods and key pair usage periods

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 requirements in Section 6.1.5 for the communicated time period.

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

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.2 Activation data protection

6.4.3 Other aspects of activation data

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

6.5.2 Computer security rating

6.6 Life cycle technical controls

6.6.1 System development controls

6.6.2 Security management controls

6.6.3 Life cycle security controls

6.7 Network security controls

6.8 Time-stamping

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

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

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

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

7.1.2 Certificate extensions

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

7.1.2.1 Root CA Certificate

a. `basicConstraints`

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

b. `keyUsage`

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

c. `certificatePolicies`

   This extension SHOULD NOT be present.

d. `extKeyUsage`

   This extension MUST NOT be present.

7.1.2.2 Subordinate CA Certificate

a. `certificatePolicies`

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

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

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

   - `certificatePolicies:policyQualifiers:policyQualifierId` (Optional)

     `id-qt 1` [RFC5280].

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

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

b. `cRLDistributionPoints`

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

c. `authorityInformationAccess`

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

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

d. `basicConstraints`

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

e. `keyUsage`

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

f. `extKeyUsage`

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

If the Subordinate CA will be used to issue Code Signing Certificates: * `id-kp-codeSigning` MUST be present. * `id-kp-timeStamping` MUST NOT be present.

If the Subordinate CA will be used to issue Timestamp Certificates: * `id-kp-timeStamping` MUST be present. * `id-kp-codeSigning` MUST NOT be present.

Additionally, the following EKUs MUST NOT be present: * `anyExtendedKeyUsage` * `id-kp-serverAuth` * `id-kp-emailProtection`

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

h. `authorityKeyIdentifier`

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

7.1.2.3 Code signing and Timestamp Certificate

a. `certificatePolicies`

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

- `certificatePolicies:policyIdentifier` (Required)

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

The following fields MAY be present:

- `certificatePolicies:policyQualifiers:policyQualifierId` (Recommended)

  `id-qt 1` [RFC 5280].

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

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

b. `cRLDistributionPoints`

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

c. `authorityInformationAccess`

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

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

d. `basicConstraints` (optional)

The `cA` field MUST NOT be true.

e. `keyUsage`

This extension MUST be present and MUST be marked critical.

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

f. `extKeyUsage`

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

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

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

Additionally, the following EKUs MUST NOT be present:

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

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

g. `authorityKeyIdentifier`

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

7.1.2.4 All Certificates

All other fields and extensions MUST be set in accordance with RFC 5280. The CA SHALL NOT issue a Certificate that contains a `keyUsage` flag, `extKeyUsage` value, Certificate extension, or other data not specified in Section 7.1.2.1, Section 7.1.2.2, or Section 7.1.2.3 unless the CA is aware of a reason for including the data in the Certificate.

CAs SHALL NOT issue a Certificate with:

a. Extensions that do not apply in the context of the public Internet (such as an extKeyUsage value for a service that is only valid in the context of a privately managed network), unless:
   i. such value falls within an OID arc for which the Applicant demonstrates ownership, or
   ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or
b. semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including an `extKeyUsage` value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.3 Algorithm object identifiers

7.1.3.1 SubjectPublicKeyInfo

As defined in Section 6.1.5.

7.1.3.2 Signature AlgorithmIdentifier

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

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

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

7.1.3.2.1 RSA

The CA SHALL use one of the following signature algorithms:

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

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

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

7.1.3.2.2 ECDSA

The CA SHALL use one of the following signature algorithms:

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

7.1.3.2.3 DSA

The CA SHALL use the following signature algorithm:

- DSA with SHA-256

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

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

7.1.4 Name forms

7.1.4.1 Name encoding

As specified in BR Section 7.1.4.1.

7.1.4.2 Subject information - Subscriber Certificates

7.1.4.2.1 Subject alternative name extension

No stipulation.

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

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

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

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

d. **Certificate Field:** Other subject attributes
Required/Optional: Optional
Contents: 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.

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

a. **Certificate Field:** `subject:organizationName` (OID 2.5.4.10)
Required/Optional: Required
Contents: The `subject:organizationName` field MUST contain either the Subject’s name or DBA as verified under BR Section 3.2. The CA MAY include

information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows “Company Name Incorporated”, the CA MAY use “Company Name Inc.” or “Company Name”. Because subject name attributes for individuals (e.g. `subject:givenName` (2.5.4.42) and `subject:surname` (2.5.4.4)) are not broadly supported by application software, the CA MAY use the `subject:organizationName` field to convey a natural person Subject’s name or DBA. The CA MUST have a documented process for verifying that the information included in the `subject:organizationName` field is not misleading to a Relying Party.

b. **Certificate Field:** `subject:streetAddress` (OID: 2.5.4.9)
Required/Optional: Optional
Contents: If present, the subject:streetAddress field MUST contain the Subject’s street address information as verified under BR Section 3.2.2.1 or 3.2.3.

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

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

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

f. **Certificate Field:** `subject:countryName` (OID: 2.5.4.6)
Required/Optional: Required
Contents: The `subject:countryName` MUST contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under BR

Section 3.2.2.3. If a Country is not represented by an official ISO 3166-1 country code, the CA MAY specify the ISO 3166-1 user-assigned code of `XX` indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

7.1.4.2.4 Subject distinguished name fields - EV Code Signing Certificates

a. **Certificate Field:** `subject:organizationName` (OID 2.5.4.10)
Required/Optional: Required
Contents: As specified in Section 9.2.1 of the EV Guidelines.

b. **Certificate Field:** `subject:businessCategory` (OID 2.5.4.15)
Required/Optional: Required
Contents: As specified in Section 9.2.3 of the EV Guidelines.

c. **Certificate Field:** sSubject Jurisdiction of Incorporation or Registration Fields
Required/Optional: Required
Contents: As specified in Section 9.2.4 of the EV Guidelines.

d. **Certificate Field:** `subject:serialNumber` (2.5.4.5)
Required/Optional: Required
Contents: As specified in Section 9.2.5 of the EV Guidelines.

e. **Certificate Field:** Subject Physical Address of Place of Business Fields
Required/Optional: Required
Contents: As specified in Section 9.2.6 of the EV Guidelines.

7.1.5 Name constraints

7.1.6 Certificate policy object identifier

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

7.1.6.1 Reserved Certificate Policy Identifiers

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

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

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

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

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

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

7.1.6.2 Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

7.1.6.3 Subordinate CA Certificates

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

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

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

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

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

1. MUST include the CA/Browser Forum reserved identifier specified in Section 7.1.6.1 to indicate the Subordinate CA's compliance with these Requirements, and

2. MAY contain the "anyPolicy" identifier (`2.5.29.32.0`) in place of an explicit policy identifier.

A Subordinate CA MUST represent, in its Certificate Policy and/or Certification Practice Statement, that all Certificates containing a policy identifier indicating compliance with these Requirements are issued and managed in accordance with these Requirements.

7.1.6.4 Subscriber Certificates

A Certificate issued to a Subscriber MUST contain one or more policy identifier(s), defined by the CA, in the Certificate's certificatePolicies extension that indicates adherence to and compliance with these Requirements. CAs complying with these Requirements MAY also assert the reserved policy OIDs in such Certificates.

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

7.1.7 Usage of Policy Constraints extension

7.1.8 Policy qualifiers syntax and semantics

7.1.9 Processing semantics for the critical Certificate Policies extension

7.2 CRL profile

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

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

7.2.1 Version number(s)

7.2.2 CRL and CRL entry extensions

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

7.3 OCSP profile

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

7.3.1 Version number(s)

7.3.2 OCSP extensions

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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

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

8.1 Frequency or circumstances of assessment

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

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

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

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

Audits MUST be conducted for all obligations under these Guidelines, including 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).

8.2 Identity/qualifications of assessor

As specified in BR Section 8.2.

8.3 Assessor's relationship to assessed entity

8.4 Topics covered by assessment

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 November 1st, 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 November 1st, 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.

8.5 Actions taken as a result of deficiency

8.6 Communication of results

As specified in BR Section 8.6.

8.7 Self-audits

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

9.1.2 Certificate access fees

9.1.3 Revocation or status information access fees

9.1.4 Fees for other services

9.1.5 Refund policy

9.2 Financial responsibility

9.2.1 Insurance coverage

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

9.2.2 Other assets

9.2.3 Insurance or warranty coverage for end-entities

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

9.3.2 Information not within the scope of confidential information

9.3.3 Responsibility to protect confidential information

9.4 Privacy of personal information

9.4.1 Privacy plan

9.4.2 Information treated as private

9.4.3 Information not deemed private

9.4.4 Responsibility to protect private information

9.4.5 Notice and consent to use private information

9.4.6 Disclosure pursuant to judicial or administrative process

9.4.7 Other information disclosure circumstances

9.5 Intellectual property rights

9.6 Representations and warranties

9.6.1 CA representations and warranties

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

1. **Compliance**. The CA and any 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 3.2 of this document, (ii) followed the procedure when issuing or managing the Certificate, and (iii) accurately described the same procedure in the CA's Certificate Policy or Certification Practice Statement.
4. **Authorization for Certificate:** At the time of issuance, the CA represents that it (i) operated a procedure for verifying that the Applicant authorized the issuance of the Certificate, (ii) followed the procedure, and (iii) accurately described the same procedure in the CA's Certificate Policy or Certification Practice Statement.
5. **Accuracy of Information:** At the time of issuance, the CA represents that it (i) operated a procedure for verifying that all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute) was true and accurate, (ii) followed the procedure, and (iii) accurately described the same procedure in the CA's Certificate Policy or Certification Practice Statement.
6. **Key Protection:** The CA represents that it provided the Subscriber at the time of issuance with documentation on how to securely store and prevent the misuse of Private Keys associated with Code Signing Certificates, or in the case of a Signing Service, securely stored and prevented the misuse of Private Keys associated with Code Signing Certificates;
7. **Subscriber Agreement:** The CA 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.

9.6.2 RA representations and warranties

9.6.3 Subscriber representations and warranties

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

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

The CA SHALL implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The CA MAY use an electronic or "click-through" Agreement provided that the

CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use. The Subscriber Agreement or Terms of Use MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information:** To provide accurate and complete information at all times in connection with the issuance of a Certificate, including in the Certificate Request and as otherwise requested by the CA.
2. **Protection of Private Key:** Where the key is available outside a Signing Service, to maintain sole control of, keep confidential, and properly protect, at all times in accordance with Section 6.2.7.4, the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token). The CA MUST provide the Subscriber with documentation on how to protect a Private Key. The CA MAY provide this documentation as a white paper or as part of the Subscriber Agreement. The Subscriber MUST represent that it will generate and operate any device storing private keys in a secure manner, as described in a document of code signing best practices, which the CA MUST provide to the Subscriber during the ordering process. The CA MUST obligate the Subscriber to use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.
3. **Private Key Reuse:** To not apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate.
4. **Use:** To use the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.
5. **Compliance with Industry Standards**: An acknowledgment and acceptance that the CA may modify the Subscriber Agreement or Terms of Use when necessary to comply with any changes in these Requirements or the Baseline Requirements.
6. **Prevention of Misuse:** To provide adequate network and other security controls to protect against misuse of the Private Key and that the CA will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys.
7. **Acceptance of Certificate:** Not to use the Certificate until after the Applicant, or an agent of Applicant, has reviewed and verified the Certificate contents for accuracy.
8. **Reporting and Revocation:** To promptly cease using a Certificate and its associated Private Key and promptly request that the CA revoke the Certificate if the Subscriber believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused or compromised, or (c) there is evidence that the Certificate was used to sign Suspect Code.

9. **Sharing of Information**: An acknowledgment and acceptance that, if: (a) the Certificate or the Applicant is identified as a source of Suspect Code, (b) the authority to request the Certificate cannot be verified, or (c) the Certificate is revoked for reasons other than Subscriber request (e.g. as a result of private key compromise, discovery of malware, etc.), then the CA is authorized to share information about the Applicant, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.
10. **Termination of Use of Certificate:** To promptly cease using the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of the Certificate.
11. **Responsiveness:** An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
12. **Acknowledgment and Acceptance:** An acknowledgement and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the Terms of Use or the Subscriber Agreement.

9.6.4 Relying party representations and warranties

9.6.5 Representations and warranties of other participants

The CA MUST contractually obligate each Signing Service to inform the CA if the Signing Service becomes aware (by whatever means) that the Signing Service has signed Suspect Code. The CA MUST require the Signing Service to request revocation of the affected Certificate and provide immediate notice to the CA if 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

9.7 Disclaimers of warranties

9.8 Limitations of liability

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

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

For Non-EV Code Signing Certificates, CAs MAY limit their liability as described in Section 9.8 of the Baseline Requirements.

9.9 Indemnities

As specified in BR Section 9.9.

9.10 Term and termination

9.10.1 Term

9.10.2 Termination

9.10.3 Effect of termination and survival

9.11 Individual notices and communications with participants

9.12 Amendments

9.12.1 Procedure for amendment

9.12.2 Notification mechanism and period

9.12.3 Circumstances under which OID must be changed

9.13 Dispute resolution provisions

9.14 Governing law

9.15 Compliance with applicable law

9.16 Miscellaneous provisions

9.16.1 Entire agreement

9.16.2 Assignment

9.16.3 Severability

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

9.16.5 Force Majeure

9.17 Other provisions

Appendix A High risk regions of concern

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

NONE