Version 1.0 Draft of Oct 18, 2013

CA/Browser Forum

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

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

Version 1.0, as adopted by the CA/Browser Forum on nn aaa nnnn.

These Baseline Requirements describe an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements that are minimum standards for the issuance and management of Code-Signing Certificates that are trusted by virtue of the fact that their corresponding Root Certificate is distributed in widely-available application software. These requirements become mandatory for all Certification Authorities issuing such certificates from a trusted root in the root store of an operating system or computer platform provider effective on the date they are incorporated into final audit criteria published by WebTrust or ETSI .

Notice to Readers

This version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates presents criteria established by the CA/Browser Forum for use by Certification Authorities when issuing, maintaining, and revoking publicly-trusted Code Signing Certificates. The Requirements may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Questions and suggestions concerning these requirements may be directed to the CA/Browser Forum at questions@cabforum.org.

The CA/Browser Forum

The CA/Browser Forum is a voluntary organization of Certification Authorities and suppliers of Internet browser and other relying-party software applications. The list of CA/Browser Forum members may be found on the following website: https://www.cabforum.org.

Other groups that have participated in the development of these Requirements include the WebTrust task force and ETSI ESI. Participation by such groups does not imply their endorsement, recommendation, or approval of the final product.

TABLE OF CONTENTS

Contents

1. Scope

The Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates describe a subset of the requirements that a Certification Authority must meet in order to issue publicly-trusted Code Signing Certificates. These Guidelines incorporate both the Baseline Requirements and the Network and Certificate System Security Requirements established by the CA/Browser Forum by reference, a copy of which may be found on the CA/Browser Forum's website at www.cabforum.org.

These Requirements do not address all of the issues that must be addressed by a CA that issues Certificates. This version of the Requirements only addresses Certificates intended to be used to digitally sign executables and scripts. 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).

2. Purpose

The primary goal of these Requirements is to enable signing of code intended for public distribution, while addressing user concerns about the trustworthiness of Certificates and the identity of the certificate holder. The Requirements also serve to inform users and help them to make informed decisions when relying on Certificates. These requirements may also help to establish the legitimacy of signed code, help to maintain the trustworthiness of software platforms, help users to make informed software choices, and limit the spread of malware. Particular software objects are not identified by a code signing certificate. Instead, only the distributor of software is identified.

3. References

As specified in the Baseline Requirements.

4. Definitions

Capitalized Terms are defined in the Baseline Requirements except where provided otherwise below:

AV Vendor: An entity that develops software used to prevent, detect, or remove malware.

CAB Forum High Risk Database: A database of information about (a) suspected or known producers, publishers, or distributors of Suspect Code; (b) Certificates revoked due to Signatures on Suspect Code or their association with fraud or other illegal conduct; and (c) Certificate requests rejected because of suspected or known fraud or other illegal conduct.

Certification Authority: An organization subject to the Requirements that is responsible for the creation, issuance, revocation, and management of Code Signing Certificates. Where the CA is also the Root CA, references to the CA will be synonymous with Root CA.

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 Signature: A Signature logically associated with a signed Object.

Code Signing Certificate: A certificate meeting the specifications contained in these Guidelines which has been issued in accordance with these Guidelines.

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

1. the identity of the person performing the verification,
2. a signed declaration by the verifying person stating that they verified the identity of the Applicant,
3. a unique identifying number from an identification document of the Applicant,
4. the date and time of the verification, and
5. a declaration of identity by the Applicant that is signed by the person performing the verification.

Issuer: A CA providing a Code Signing Certificate to a Subscriber or a Signing Authority that provides a Signature for an Object submitted to it by the Subscriber.

Individual Applicant: An Applicant that is an individual and requests a Certificate that will list the Applicant's legal name as the Certificate subject.

Object: A contiguous set of bits that has been or can be digitally signed with a private key that corresponds to a Code Signing Certificate. Also referred to herein as Code.

Organizational Applicant: An Applicant that requests a Certificate subject other than the name of an individual. Organizational Applicants include private and public corporations, LLCs, partnerships, government entities, non-profit organizations, trade associations, and other entities.

Requirements: This document, the Baseline Requirements, and the Network and Certificate System Security 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 Authority: An organization that signs an Object on behalf of a Subscriber.

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

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.

Timestamp Authority: An organization that timestamps data, thereby asserting that the data existed at the specified time;

5. Abbreviations and Acronyms

As specified in the Baseline Requirements.

6. Conventions

Terms not otherwise defined in these Guidelines shall be as defined in applicable agreements, user manuals, Certificate Policies and Certification Practice Statements, of the CA.

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

7. Certificate Warranties and Representations

7.1 By the CA and Root CA

By issuing a Certificate, the CA and its Root CA make the Certificate Warranties listed below to the Certificate Beneficiaries listed below.

7.1.1 Certificate Beneficiaries

Certificate Beneficiaries include the following:

1. The Subscriber entering into the Subscriber Agreement for the Certificate;

2. 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

3. All Relying Parties who reasonably rely on such Certificate while a Signature associated with the Certificate is valid.

7.1.2 Certificate Warranties

The CA and its Root CA represent to the Certificate Beneficiaries that:

1. **Compliance**. During the period when a Signature is valid, the CA has complied with these Requirements and its Certificate Policy and Certification Practice Statement in issuing each Code Signing Certificate.

2. **Identity of Subscriber**: That, at the time of issuance the CA operated a procedure for verifying the identity of the Subscriber that at least meets the requirements in Section 11;

the procedure was followed, and the same procedure was accurately described in the CA's Certificate Policy and Certification Practice Statement;

3. **Authorization for Certificate:** That, at the time of issuance: (i) the CA operated a procedure for validating that the Applicant authorized the issuance of the Certificate; (ii) the procedure was followed; and (iii) the same procedure was accurately described in the CA's Certificate Policy and Certification Practice Statement;

4. **Accuracy of Information:** That, at the time of issuance: (i) the CA operated a procedure for validating that all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute) was true and accurate; (ii) the procedure was followed; and (iii) the same procedure was described in the CA's Certificate Policy and Certification Practice Statement;

5. **Security Awareness:** That, at the time of issuance the CA required the Subscriber to securely store and prevent the misuse of Private Keys associated with Code Signing Certificates;

6. **Subscriber Agreement:** That the Applicant has entered into a legally valid and enforceable Subscriber Agreement with the CA that satisfies these Requirements;

7. **Status:** That the CA will maintain a 24 x 7 online-accessible Repository with current information regarding the status of all unexpired Certificates as valid or revoked; and

8. **Revocation:** That the CA will revoke a Certificate upon the occurrence of any Revocation Event as specified in these Requirements.

7.2 By the Applicant

The CA MUST require, as part of the Subscriber Agreement, that the Applicant make the commitments and warranties set forth in Section 10.3.2 of these Requirements, for the benefit of the CA and the Certificate Beneficiaries.

8. Community and Applicability

8.1 Compliance

The CA and its Root CA MUST at all times:

1. Comply with all laws applicable to its business and the Certificates it issues in each jurisdiction where it operates;

2. Comply with these Requirements;

3. Comply with the audit requirements set forth in Section 17; and

4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

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 SHALL notify the CA / Browser Forum of the facts, circumstances, and law(s) involved, so that the CA/Browser Forum may revise these Requirements accordingly.

8.2 Certificate Policies

8.2.1 Implementation

The CA and its Root CA MUST develop, implement, enforce, display prominently on its Web site, and periodically update its policies and practices, including its Certificate Policy and Certification Practice Statement that implement these Requirements as they may be revised from time-to-time.

With the exception of revocation checking for time-stamped and expired certificates, platforms are expected to validate Code Signatures in accordance with RFC 5280. When a platform encounters a certificate that fails to validate due to revocation, the platform should reject the code. When a platform encounters a certificate that fails to validate for reasons other than revocation, the platform should treat the code as it would if it had been unsigned.

Ordinarily, a Code Signature created by a Subscriber may be considered valid for an indefinite period after expiration of the Certificate. However, the “Timestamp” method and the “Signing Authority” method provide greater assurance in the Code Signature:

1. Timestamp Method: In this method, the Subscriber signs the code, appends its Code Signing Certificate and submits it to a Timestamp Authority to be time-stamped. The resulting package can be considered valid up to the expiration time of the timestamp certificate (which may be up to one hundred and twenty three months in the future).

2. Signing Authority Method: In this method, the Subscriber submits the code, or a digest of the code, to a Signing Authority for signature. The resulting signature is valid up to the expiration time of the Signing Authority certificate (which may be up to one hundred and twenty three months in the future).

8.2.2 Disclosure

The CA and its Root CA MUST publicly disclose their policies and practices through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA is also REQUIRED to publicly disclose its CA business practices such as are required to be publicly disclosed by the audit scheme (see Section **Error! Reference source not found.**). The disclosures MUST be structured in accordance with either RFC 2527 or RFC 3647.

8.3 Commitment to Comply

The CA and its Root CA MUST publicly give 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 Code Signing Requirements published at http://www.cabforum.org. If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

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

8.4 Trust model

The CA SHALL disclose all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

9. Certificate Content and Profile

9.1 Issuer Information

As specified in Section 9.1 of the Baseline Requirements.

9.2 Subject Information

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

9.2.1 Subject Alternative Name Extension

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

9.2.2 Subject Common Name Field

Certificate Field: subject:commonName (OID 2.5.4.3)

Required/Optional: Optional

Contents: Subject's legal name as verified under Section 11.2.

9.2.3 Subject Domain Component Field

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

9.2.4 Subject Distinguished Name Fields

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 Section 11.2. The CA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name". Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, the CA MAY use the subject:organizationName field to convey a natural person Subject's name or DBA.

b. **Certificate Field**: Number and street: subject:streetAddress (OID: 2.5.4.9)

Required/Optional: Optional if the subject:organizationName field is present.

Contents: If present, the subject:streetAddress field MUST contain the Subject's street address information as verified under Section 11.2.

c. **Certificate Field**: subject:localityName (OID: 2.5.4.7)

Required/Optional: Required if the subject:organizationName field is present and the subject:stateOrProvinceName field is absent. Required if the subject:organizationName field is present and the subject:stateOrProvinceName field is absent. Optional if the subject:organizationName and subject:stateOrProvinceName fields are present.

Contents: If present, the subject:localityName field MUST contain the Subject's locality information as verified under Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 9.2.5, the localityName field MAY contain the Subject's locality and/or state or province information as verified under Section 11.2.

d. **Certificate Field**: subject:stateOrProvinceName (OID: 2.5.4.8)

Required/Optional: Required if the subject:organizationName field is present and subject:localityName field is absent. Optional if subject:organizationName and subject:localityName fields are present.

Contents: If present, the subject:stateOrProvinceName field MUST contain the Subject's state or province information as verified under Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 9.2.5, the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information as verified under Section 11.2.5.

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 Section 11.2

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 Section 11.2. If a Country is not represented by an official ISO 3166-1 country code, the CA MAY specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

9.2.5 Reserved

9.2.6 Subject Organizational Unit Field

Certificate Field: subject:organizationalUnitName

Required/Optional: Optional.

Contents: The CA SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 11.2.

9.2.7 Other Subject Attributes

As specified in Section 9.2.7 of the Baseline Requirements.

9.3 Certificate Policy Identification

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

9.3.1 Subscriber Certificates

The following Certificate Policy Identifier is reserved for use by CAs as an optional means of asserting compliance with these Requirements as follows:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) code signing(3)} (2.23.140.1.2.3)

9.3.2 Root CA Requirements

As specified in Section 9.3.2 of the Baseline Requirements.

9.3.3 Subordinate CA Certificates

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

1. MUST include one or more explicit policy identifiers that indicates the Subordinate CA's adherence to and compliance with these Requirements (i.e. either the CA/Browser Forum reserved identifiers or identifiers defined by the CA in its Certificate Policy and/or Certification Practice Statement) and

2. MUST NOT contain the "anyPolicy" identifier (2.5.29.32.0).

A Certificate issued after the Effective Date to a Subordinate CA that is an affiliate of the Issuing CA:

1. MAY include the CA/Browser Forum reserved identifiers or an identifier defined by the CA in its Certificate Policy and/or Certification Practice Statement 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 SHALL represent, in its Certificate Policy and/or Certification Practice Statement, that all Certificates containing a policy identifier indicating compliance with these Requirements are issued and managed in accordance with these Requirements.

9.3.4 Subscriber Certificates

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

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

9.4 Maximum Validity Period

Code may be signed at any point in the development or distribution process, either by a software publisher or a user organization. Signed code 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 MUST NOT exceed one hundred and twenty-three months. The validity period for a Code Signing Certificate issued to a Signing Authority that fully complies with the Requirements MUST NOT exceed one hundred and twenty-three months. The validity period for a Timestamp Certificate issued to a Timestamp Authority that fully complies with these Requirements MUST NOT exceed one hundred and twenty-three months.

9.5 Subscriber Public Key

As specified in Section 9.5 of the Baseline Requirements.

9.6 Certificate Serial Number

As specified in Section 9.6 of the Baseline Requirements.

9.7 Other Technical Requirements

As specified in Section 9.7 of the Baseline Requirements.

10. Certificate Request

10.1 Documentation Requirements

As specified in Section 10.1 the Baseline Requirements.

10.2 Certificate Request Requirements

10.2.1 General

As specified in Section 10.2.1 of the Baseline Requirements.

10.2.2 Request and Certification

As specified in Section 10.2.2 of the Baseline Requirements.

10.2.3 Information Requirements

As specified in Section 10.2.3 of the Baseline Requirements.

10.2.4 Subscriber Private Key

If the CA or any of its designated RAs generated the Private Key on behalf of the Subscriber, then the CA SHALL encrypt the Private Key for transport to the Subscriber.

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

10.3 Subscriber Agreement

10.3.1 General

As specified in Section 10.3.1 of the Baseline Requirements.

10.3.2 Agreement Requirements

CAs MUST impose the following obligations and warranties on each Applicant (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) using a Subscriber or Terms of Use Agreement:

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:** To take reasonable measures to maintain sole control of, keep confidential, and properly protect, at all times, the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);

3. **Use:** To use the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign malicious code or any code that is downloaded without consent and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement;

4. **Prevention of Misuse:** To provide adequate network and other security controls to protect against misuse of the Private Key.

5. **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;

6. **Reporting and Revocation:** To promptly cease using a Certificate and its associated Private Key and promptly request that the CA revoke the Certificate if (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key contained in the Certificate, or (c) there is evidence that the Certificate was used to sign Suspect Code;

7. **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, application, Certificate, or surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.

8. **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; and

9. **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 or if the CA discovers that the Certificate is being used in illegal activity such as phishing, fraud, malware distribution, etc.

10.3.3 Service Agreement Requirements for Signing Authorities

If a Signing Authority becomes aware (by whatever means) that it has signed code that contains malicious software or a serious vulnerability, then it MUST immediately inform the issuing CA. If a Signing Authority's private key, or private key activation data, is compromised or believed to be compromised, the Signing Authority MUST contact the issuing CA immediately and request that the certificate be revoked.

Signing Authorities must obtain the Subscriber's legally enforceable 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 signature that contains Suspect Code; and

3. Inform the Signing Authority if it is discovered (by whatever means) that code submitted to the Signing Authority for signature contained malware or a serious vulnerability.

11. Verification Practices

11.1 Overview

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

1. Verify the Subject's legal identity, including any DBA included in a Certificate,

2. Verify the Subject's address, and

3. Verify the Certificate Requester's authority to request a certificate and the authenticity of the Certificate request using a verified method of communication.

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

1. Verify the Subject's identity using a government photo ID,

2. Verify the Subject's address using reliable data sources,

3. Obtain either a biometric associated with the Subject, such as a fingerprint, or signed Declaration of Identity,

4. Verify the Certificate Requester's authority to request a certificate and the authenticity of the Certificate request using a verified method of communication.

11.2 Verification of Subject Identity Information

11.2.1 Identity

As specified in Section 11.2.1 of the Baseline Requirements.

11.2.2 DBA/Tradename

As specified in Section 11.2.2 of the Baseline Requirements.

11.2.3 Authenticity of Certificate Request

As specified in Section 11.2.3 of the Baseline Requirements.

11.2.4 Verification of Individual Applicant

The CA SHALL verify the Applicant's name using:

1. A legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The CA SHALL inspect the copy for any indication of alteration or falsification AND

2. Either a fully executed Declaration of Identity, the authenticity of which is confirmed with the verifying person using a Reliable Method of Communication, or at least one unique biometric identifier (such as a fingerprint or handwritten signature) that is obtained in-person through a Delegated Third Party.

The CA SHALL verify the Applicant's address using a form of identification that the CA determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. The CA MAY rely on the same government-issued ID that was used to verify the Applicant's name.

The CA SHALL verify the certificate request with the Applicant using a Reliable Method of Communication.

11.3 Age of Certificate Data

As specified in Section 11.3 of the Baseline Requirements.

11.4 Denied List

As specified in Section 11.4 of the Baseline Requirements.

11.5 High Risk Requests

In addition to the procedures required by Section 11.5 of the Baseline Requirements, prior to issuing a Code Signing Certificate each CA SHALL evaluate the risks of certificate issuance (i.e. potential fraud, malware signing, or other illegal activity), by checking databases of information about the following:

a. suspected or known producers, publishers, or distributors of Suspect Code and

b. certificates revoked due to Signatures on Suspect Code;.

The CAB Forum High Risk Database is deemed to meet these database requirements.

If a certificate request is rejected due to risk of issuance described above, then the CA MAY provide all relevant information and risk indicators to the CAB Forum High Risk Database. The CA MAY remain anonymous for such submissions.

11.6 Data Source Accuracy

As specified in Section 11.6 of the Baseline Requirements.

12. Certificate Issuance by a Root CA

As specified in Section 12 of the Baseline Requirements.

13. Certificate Revocation and Status Checking

13.1 Revocation

13.1.1 Revocation Request

As specified in Section 13.1.1 of the Baseline Requirements.

13.1.2 Certificate Problem Reporting

The CA SHALL provide AV Vendors, Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, Certificates used to sign Suspect Code, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA SHALL publicly disclose the instructions through a readily accessible online means.

The CA SHALL respond to all plausible notices that Suspect Code verifies with a certificate that it has issued.

13.1.3 Investigation

The CA SHALL 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 complaint (for example, a complaint from an AV Vendor or law enforcement agency carries more weight than an anonymous complaint); and
4. Relevant legislation.

13.1.4 Response

The CA SHALL maintain a continuous 24x7 ability to communicate with AV Vendors, Application Software Suppliers, and law enforcement agencies and to respond to high-priority Certificate Problem Reports it receives, such as those involving malicious code, fraud, or other illegal conduct, and to revoke the Certificate.

13.1.5 Reasons for Revoking a Subscriber Certificate

The CA SHALL revoke a Code Signing Certificate within 24 hours if one or more of the following occurs:

1. 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;

2. The CA obtains evidence that the Subscriber’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (also see Section 10.3.2);

3. The CA obtains evidence that the Certificate was misused, including any use of a Certificate to sign Suspect Code;

4. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;

5. The CA is made aware of a material change in the information contained in the Certificate or that any information appearing in the Certificate is inaccurate or misleading;

6. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;

7. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

8. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;

9. The CA is made aware of a possible compromise of the Private Key of a CA used for issuing the Certificate;

10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or

11. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

A CA revoking a Certificate because it has been associated with signing of Suspect Code or other fraudulent or illegal conduct SHOULD provide all relevant information and risk indicators to other CAs or industry groups, including the CAB Forum.

13.1.6 Reasons for Revoking a Subordinate CA Certificate

As specified in Section 13.1.6 of the Baseline Requirements.

13.2 Certificate Status Checking

In addition to Section 13.2 of the Baseline Requirements, CAs SHALL provide accurate and up-to-date revocation status information for at least one year beyond expiry of the Code Signing Certificate.

Whenever practical, platforms should check the revocation status of the certificates that they rely upon. However, this is not always practical, such as when signed code is loaded earlier in the boot sequence than the network communication stack.

In the timestamp model, the platform should deviate from the RFC 5280 certification path validation algorithm and check the revocation status, not only of the timestamp certificate, but also of the Subscriber's Code Signing Certificate at the time of reliance rather than at the time the time-stamp was applied. In addition to checking revocation status, where practical, platforms should consult blacklists of suspect software.

A certificate may have a one-to-one relationship with the software object that it verifies. In such cases, revocation of the certificate only invalidates the signature on the code that is suspect. If, on the other hand, a certificate has a one-to-many relationship with the software objects that it verifies, then revocation of the certificate invalidates the signatures on all those software objects, some of which may be perfectly sound.

14. Employees and Third Parties

14.1 Trustworthiness and Competence

As specified in Section 14.1 of the Baseline Requirements.

14.2 Delegation of Functions to Registration Authorities and Subcontractors

14.2.1 General

Except as stated in Section 14.2.2, the CA MAY delegate the performance of all, or any part, of Section 11 of these Requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 10.3.3.

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

1) Meet the qualification requirements of Section 14.1 of the Baseline Requirements, when applicable to the delegated function;
2) Retain documentation in accordance with Section 15 of the Baseline Requirements;
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 SHALL verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 and the document retention and event logging requirements of Section 15.

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

14.2.2 Enterprise RAs

The CA MAY designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization.

14.2.3 Compliance Obligation

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

14.2.4 Responsibility

As specified in Section 14.2.4 of the Baseline Requirements.

15. Data Records

As specified in Section 15 of the Baseline Requirements.

16. Data Security and Private Key Protection

As specified in Section 16 of the Baseline Requirements. Systems used to process and approve Code Signing Certificate requests MUST require actions by at least two trusted persons before creating a Code Signing Certificate. In addition, effective January 1, 2015:

1. A Timestamp Authority MUST protect its Private Key in a crypto module validated in accordance with FIPS 140 Level 2, Common Criteria EAL 4+ (ALC_FLR.2), or equivalent.

2. An Timestamp Authority MUST be synchronized with a UTC(k) time source recognized by the International Bureau of Weights and Measures (BIPM).

3. Signing Authorities shall protect private keys in a in a crypto module validated in accordance with FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent. Techniques that may be used to satisfy this requirement include:

    a. Use of an HSM in a multi-tenancy solution protected by two-factor authentication;

    b. A hardware crypto module provided by the CA;

    c. Installation directly to a hardware crypto module by the CA;

    d. Contractual terms in a Subscriber Agreement / Terms of Use requiring the Subscriber to protect the private key as required above and with compliance being confirmed by written attestation of an independent third party; or

    e. the Signing Authority uses a documented process to verify protection of the private key that provides a level of assurance equivalent to the processes listed above.

4. CAs SHALL ensure that the Subscriber's private key is generated, stored and used in Secure Signature Creation Device or a crypto module that meets or exceeds the requirements of FIPS 140 level 2, EAL 4+, or equivalent.

Acceptable methods of satisfying this requirement include:

a. The CA ships a suitable hardware crypto module, with a preinstalled key pair and corresponding certificate, in the form of a smartcard or USB device or similar and with the activation data sent separately to the Subscriber;

b. The CA uses a process that remotely installs the private key or remotely verifies the installation of a private key on a FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent device and then provides the corresponding Certificate;

c. The CA or RA stores the private key on an HSM that meets or exceeds FIPS 140-2 Level 2 and permits the Subscriber to access or use the private key through a multi-tenancy solution that is protected using multi-factor authentication;

d. The Subscriber provides a report from a qualified independent third party (a CISA or auditor with IT training and experience) indicating that the Subscriber key storage and usage achieves a level of security at least equivalent to that of FIPS 140 level 2 or Common Criteria EAL 4+. The CA MUST verify the authenticity of the audit report; or

e. The CA follows a documented process to verify protection of the private key that provides a level of assurance equivalent to the processes listed above.

17. Audit

As specified in Section 17 the Baseline Requirements.

18. Liability and Indemnification

As specified in Section 18 of the Baseline Requirements.

Appendix A

Minimum Cryptographic Algorithm and Key Size Requirements

As specified in the Baseline Requirements.

Appendix B

Certificate Extensions (Normative)

This appendix specifies the requirements for extensions in Certificates.

(1) Root CA Certificates

As specified in Appendix A of the Baseline Requirements.

(2) Subordinate CA Certificates

A. certificatePolicies

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

certificatePolicies:policyIdentifier (Required)

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

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

certificatePolicies:policyQualifiers:policyQualifierId

- id-qt 1 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier:cPSuri

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

B. cRLDistributionPoint

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

D. basicConstraints

This extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The cA field MUST be set true. The pathLenConstraint field MAY be present.

E. keyUsage

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

All other fields and extensions SHALL be set in accordance to RFC 5280.

(3) Subscriber Certificates

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.

certificatePolicies:policyQualifiers:policyQualifierId (Recommended)

- id-qt 1 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

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

B. cRLDistributionPoint

C. This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA’s CRL service.

D. authorityInformationAccess

E. This extension MUST be present and MUST NOT be marked critical. The extension MUST contain the HTTP URL of the CA’s OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL for the Root CA’s certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

F. basicConstraints (optional)

If present, the cA field MUST be set false.

G. keyUsage (required)

This extension MUST be present and MUST be marked critical. The bit positions for digitalSignature MUST be set. All other bit positions SHOULD NOT be set.

H. extKeyUsage (required)

The value id-kp-codeSigning [RFC5280] MUST be present. The value anyExtendedKeyUsage (2.5.29.37.0) MUST NOT be present. Other values SHOULD NOT be present.

All other fields and extensions SHALL be set in accordance to RFC 5280.

Appendix C

User Agent Verification (Normative)

As specified in Appendix C of the Baseline Requirements

Appendix D

Sample Applicant Quiz (Illustrative)

Your code signing certificate and associated key pair are very valuable assets.

Your private key, like any other valuable asset, may be targeted by thieves who may try to steal it or get you to misuse it for illegal purposes.

Therefore, before proceeding, we ask that you take the following quiz:

	True or False	Tell me more…
Code signing keys are valuable targets for criminals who may try to steal or misuse them.	True	Links
The theft or misuse of your code signing key will not result in revocation of your certificate. It is unlikely that revocation of your code signing certificate will adversely affect your customers.	False	Links
You should implement strong access controls to protect your signing keys and the machines that house them so that they may only be used by trusted persons.	True	Links
The machine that you use to sign code does not need to be patched or protected with good computer hygiene, such as anti-virus and malware scans, firewalls, etc.	False	Links
The machine that you use to sign code should not be connected to the Internet unless it is fully protected.	True	Links
You may store your private signing key(s) anywhere you'd like, including a plain text file on your main desktop screen. We strongly recommend that your signing keys be stored in a certified cryptographic module, token, or hardware appliance.	False	Links
It is a risk mitigation practice to use two or more key sets (e.g. development, production/public release, backup, etc.) in order to segregate and mitigate your risk in case one of your keys is compromised.	True	Links
It is acceptable to sign and distribute code that you have not checked, even though it may have viruses.	False	Links