Version 1.2

CA/Browser Forum

Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates

A request to make a translated version of these Guidelines should be submitted to questions@cabforum.org.

Notice to Readers

The Guidelines for the Issuance and Management of Extended Validation Code Singing Certificates present criteria established by the CA/Browser Forum for use by certification authorities when issuing, maintaining, and revoking certain digital certificates for use in signing digital objects. These Guidelines may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Questions or suggestions concerning these guidelines may be directed to the CA/Browser Forum at questions@cabforum.org.

Document History

Ver.	Ballot	Description	Adopted	Effective*
1.1	72	Reorganize EV Documents	29 May 2012	29 May 2012
1.2	117	EV Code Signing Guidelines Corrections	24 Mar 2014	24 Mar 2014

The CA/Browser Forum

The CA/Browser Forum is a voluntary open organization of certification authorities and suppliers of Internet browsers and other relying-party software applications.

Table of Contents

1 Scope

These Guidelines describe the minimum requirements that apply to the issuance of Extended Validation Code Signing Certificates and EV signatures. Certification Authority, Timestamp Authority and Signing Authority are all governed by these Guidelines. The Timestamp Authority and the Signing Authority are optional components of the environment. The Guidelines incorporate by reference the Baseline Requirements and EV Guidelines as adopted by the CA/Browser Forum. The most recent versions of these two documents are available on the CA/Browser Forum's website at http://cabforum.org/documents.html and apply equally to EV Code Signing Certificates except where stated otherwise herein.

These Guidelines do not acknowledge gradations of assurance in code; they simply define one level of assurance.

Subject Organization information from Valid EV Code Signing Certificates may be displayed in a special manner by certain relying-party software applications in order to provide users with a trustworthy confirmation of the identity of the entity providing the code signing services.

These Guidelines address the basic issue of validating Subject identity information in EV Code Signing Certificates and some related matters. They do not address all of the related matters, such as certain technical and operational ones.

These Guidelines do not address the verification of information, or the issuance, use, maintenance, or revocation of EV Code Signing Certificates by enterprises that operate their own Public Key Infrastructure for internal purposes only, where its Root CA Certificate is not distributed by any Application Software Supplier.

2 Purpose

2.1 Purpose of EV Code Signing Certificates

EV Code Signing Certificates and signatures are intended to be used to verify the identity of the certificate holder (Subscriber) and the integrity of its code. They provide assurance to a user or platform provider that code verified with the certificate has not been modified from its original form and is distributed by the legal entity identified in the EV Code Signing Certificate by name, Place of Business address, Jurisdiction of Incorporation or Registration, and other information. EV Code Signing Certificates may 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.

No particular software object is identified by an EV Code Signing Certificate, only its distributor is identified.

2.1.1 Secondary Purposes

As specified in Section 2.1.1 of the EV Guidelines.

2.1.2 Excluded Purposes

EV Code Signing Certificates focus only on assuring the identity of the Subscriber and that the signed code has not been modified from its original form. EV Code Signing Certificates are ***not*** intended to provide any other assurances, representations, or warranties. Specifically, EV Code Signing Certificates do not warrant that code is free from vulnerabilities, malware, bugs, or other problems. EV Code Signing Certificates do not warrant or represent that:

i) The Subject named in the EV Code Signing Certificate is actively engaged in doing business;

ii) The Subject named in the EV Code Signing Certificate complies with applicable laws;

iii) The Subject named in the EV Code Signing Certificate is trustworthy, honest, or reputable in its business dealings; or

iv) It is "safe" to install code distributed by the Subject named in the EV Code Signing Certificate.

3 References

See the most recent version of the Baseline Requirements and EV Guidelines, available on the CA/Browser Forum's website at http://cabforum.org/documents.html.

4 Definitions

Capitalized Terms are defined in the Baseline Requirements and EV Guidelines unless provided otherwise below:

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

EV Code Signing Object: An EV Code Signing Certificate issued by a CA or an EV Signature provided by a Signing Authority.

EV 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.

Certification Authority: An organization agreeing to be bound by these Guidelines that is responsible for the creation, issuance, revocation, and management of EV Code Signing Certificates. Where the CA is also the Root CA, references to the CA will be synonymous with Root CA.

Issuer: A CA providing an EV Code Signing Certificate to a Subscriber or a Signing Authority that provides an EV signature for a Subscriber.

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

Signing Authority: An organization that signs code on behalf of a Subscriber.

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

5 Abbreviations and Acronyms

Abbreviations and Acronyms are defined in the Baseline Requirements and EV Guidelines.

6 Conventions

As specified in the EV Guidelines.

7 Certificate Warranties and Representations

7.1 EV Code Signing Certificate Warranties

When a CA issues an EV Code Signing Certificate, the CA and its Root CA represents and warrants to the Certificate Beneficiaries listed in Section 7.1.1 of the Baseline Requirements, during the period when the EV Code Signing Certificate is Valid, that the CA has followed the requirements of these Guidelines and its EV Policies in issuing and managing the EV Code Signing Certificate and in verifying the accuracy of the information contained in the EV Code Signing Certificate. Similarly, when a Signing Authority provides an EV Signature, the Signing Authority represents and warrants to the Certificate Beneficiaries listed in Section 7.1.1 of the Baseline Requirements, during the period when the EV Signature is Valid, that the CA has followed the requirements in providing the EV Signature to the Subscriber. These warranties specifically include, but are not limited to, the following:

(A) **Legal Existence:** The Issuer 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 Object was issued, the Subject of the EV Code Signing Object legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;

(B) **Identity:** The Issuer has confirmed that, as of the date the EV Code Signing Object was issued, the legal name of the Subject named in the EV Code Signing Object matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;

(C) **Authorization for EV Code Signing Certificate:** The Issuer has taken all steps reasonably necessary to verify that the Subject of the EV Code Signing Object authorized the issuance of the EV Code Signing Object;

(D) **Accuracy of Information:** The Issuer has taken all steps reasonably necessary to verify that all of the other information in the EV Code Signing Object is accurate, as of the date of issuance;

(E) **Subscriber Agreement:** The Subject of the EV Code Signing Object has entered into a legally valid and enforceable Subscriber Agreement with the Issuer that satisfies the requirements of these Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;

(F) **Status:** The Issuer will follow the requirements of these Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Code Signing Object as Valid or revoked; and

(G) **Revocation:** The Issuer will follow the requirements of these Guidelines and revoke the EV Code Signing Object for any of the revocation reasons specified in these Guidelines.

7.2 By the Applicant

Applicants make the commitments and warranties set forth in Section 10.3.2 of these Guidelines for the benefit of the Issuer and the Certificate Beneficiaries.

8 Community and Applicability

8.1 Issuance of EV Code Signing Certificates

Issuers MAY issue EV Code Signing Certificates, provided that the Issuer (and any Root CA) satisfy the requirements in these Guidelines and the Baseline Requirements

If a court or government body with jurisdiction over the activities covered by these Guidelines 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 Guidelines accordingly.

8.2 EV Code Signing Policies

8.2.1 Implementation

Each Issuer MUST develop, implement, enforce, display prominently on its Web site, and periodically update as necessary its own auditable EV Code Signing Object practices, policies and procedures, such as a Certification Practice Statement (CPS) and Certificate Policy (CP) that:

(A) Implement the requirements of these Guidelines as they are revised from time-to-time;

(B) Implement the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program or ETSI TS 102 042 V2.1.1; and

(C) Specify the Issuer's (and applicable Root CA's) entire root certificate hierarchy including all roots that its EV Code Signing Certificates depend on for proof of those EV Code Signing Certificates' authenticity.

With the exception of revocation checking for time-stamped and expired certificates, platforms are expected to validate signed code 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 a period of up to thirty-nine months. However, a code signature may be treated as valid for a period of up to one hundred and twenty three months by means of one of the following methods: the "Timestamp" method or the "Signing Authority" method.

(A) Timestamp Method: In this method, the Subscriber signs the code, appends its EV Code Signing Certificate (whose expiration time is less than thirty-nine months in the future) and submits it to an EV 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).

(B) Signing Authority Method: In this method, the Subscriber submits the code, or a digest of the code, to an EV 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

Each Issuer MUST publicly disclose their EV Policies through an appropriate and readily accessible online means that is available on a 24x7 basis. The Issuer is also REQUIRED to publicly disclose its CA business practices as required by either WebTrust for CAs or ETSI TS 102 042 V2.1.1. The disclosures MUST be structured in accordance with either RFC 2527 or RFC 3647.

8.3 Commitment to Comply with Recommendations

Each Issuer SHALL publicly give effect to these Guidelines and represent that they will adhere to the latest published version by incorporating them into their respective EV Policies, using a clause such as the following (which must include a link to the official version of these Guidelines):

> [Name of Issuer] conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Code Signing Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

In addition, the Issuer MUST include (directly or by reference) the applicable requirements of these Guidelines in all contracts that involve or relate to the issuance or maintenance of EV Code Signing Certificates. The Issuer MUST enforce compliance with such terms.

8.4 Insurance

Issuers must meet the requirements and abide by the obligation in Section 8.4 of the EV Guidelines.

8.5 Obtaining EV Code Signing Certificates

Issuers MAY only issue EV Code Signing Objects to Applicants that meet the requirements specified in Section 8.5 of the EV Guidelines.

9 EV Certificate Content and Profile

9.1 Issuer Information

Issuer information listed in an EV Code Signing Object MUST comply with Section 9.1 of the Baseline Requirements.

9.2 Subject Information

EV Code Signing Objects issued to Subscribers MUST include the following information about the Subject organization in the fields listed:

9.2.1 Subject Organization Name Field

As specified in Section 9.2.1 of the EV Guidelines.

9.2.2 Subject Alternative Name Extension

This field MUST be present and MUST contain the permanentIdentifier specified in Section 9.7. This field MUST NOT contain a Domain Name or IP Address.

9.2.3 Subject Common Name Field

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 11.2.

9.2.4 Subject Business Category Field

As specified in Section 9.2.4 of the EV Guidelines.

9.2.5 Subject Jurisdiction of Incorporation or Registration Field

As specified in Section 9.2.5 of the EV Guidelines.

9.2.6 Subject Registration Number Field

As specified in Section 9.2.6 of the EV Guidelines.

9.2.7 Subject Physical Address of Place of Business Field

As specified in Section 9.2.7 of the EV Guidelines.

9.2.8 Other Subject Attributes

All other optional attributes, when present within the subject field, MUST contain information that has been verified by the Issuer. Optional subfields within the Subject field MUST either contain information verified by the Issuer or MUST be left empty. Metadata such as '.', '-', and ' ' characters, and/or any other indication that the field is empty, absent or incomplete, MUST not be used.

9.3 Certificate Policy Identification

As specified in Section 9.3 of the EV Guidelines.

9.4 Maximum Validity Period For EV Code Signing Certificate

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.

Subscribers may obtain an EV Code Signing Certificate with a validity period not exceeding thirty-nine months.

Timestamp Authorities and Signing Authorities may obtain an EV Timestamp Certificate or EV Code Signing Certificate (respectively) with a validity period not exceeding one hundred and twenty three months.

The validity period for an EV Code Signing Certificate issued to a Subscriber MUST NOT exceed thirty-nine months. The validity period for an EV Code Signing Certificate issued to a Signing Authority that fully complies with these Guidelines MUST NOT exceed one hundred and twenty three months. The validity period for an EV Timestamp Certificate issued to a Timestamp Authority that fully complies with these Guidelines MUST NOT exceed one hundred and twenty three months.

9.5 Subscriber Public Key

As specified in Section 9.5 of the EV Guidelines.

9.6 Certificate Serial Number

As specified in Section 9.6 of the EV Guidelines.

9.7 Additional Technical Requirements for EV Code Signing Certificates

As specified in Section 9.7 of the EV Guidelines, with the following exceptions:

(A) the Domain Name required by Section 8.1.1(2) SHALL be omitted;

(B) the Certificate MUST include a SubjectAltName:permanentIdentifier which MUST contain the following:

1) The ISO 3166-2 country code corresponding Subject's Jurisdiction of Incorporation or Registration (CC), as specified in the subject:jurisdictionOfIncorporationCountryName field;

2) If applicable, the state, province, or locality of the Subject's Jurisdiction of Incorporation in uppercase characters as specified in the subjectjurisdictionOfIncorporationLocalityName or subject:jurisdictionofIncorporationStateorProvinceName field, expressed in an unabbreviated format (STATE);

3) The first one of the following that applies:

a. The Registration Number as included in the Subject:serialNumber field (REG),

b. A date of Incorporation or Registration in YYYY-MM-DD format (DATE) and the Subject's Organization Name as included in the organizationName field (ORG),

c. A verifiable date of creation in YYYY-MM-DD format (DATE) and the Subject's Organization Name as included in the organizationName field (ORG), or

d. the Subject's Organization Name as included in the organizationName field (O).

The CA SHALL format data in the SubjectAltName:permanentIdentifier extension using Unicode as follows: CC-STATE (if applicable)- REG or DATE (if available)-ORG (if REG is not present). Characters representing the organization name MUST be uppercase Unicode. Any included "-" characters MUST be Unicode 002D and any included spaces in REG, STATE, or ORG MUST be Unicode 0020.

A CA MAY truncate or abbreviate an organization name included in this field to ensure that the combination does not exceed 64 characters provided that the CA checks this field in accordance with section 10.11.1 and a Relying Party will not be misled into thinking that they are dealing with a different organization. If this is not possible, the CA MUST NOT issue the EV Code Signing Certificate.

(C) the keyUsage extension MUST be set as follows:

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

(D) the extended keyUsage extension MUST be set as follows:

This extension MUST be present, and the value id-kp-codeSigning MUST be present. Other values SHOULD NOT be present.

10 EV Code Signing Certificate Request Requirements

10.1 General Requirements

As specified in Section 10.1 of the EV Guidelines.

10.2 EV Code Signing Certificate Request Requirements

As specified in Section 10.2 of the EV Guidelines.

10.3 Requirements for Subscriber Agreement and Terms of Use

10.3.1 General

Prior to issuing an EV Code Signing Object, the Issuer SHALL obtain, for the express benefit of the Issuer and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the Issuer, or
2. The Applicant's agreement to the Terms of Use agreement.

The Issuer SHALL implement a process to ensure that each Subscriber or Terms of Use Agreement is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the EV Code Signing Object to be issued pursuant to the certificate request. The Issuer MAY use an electronic or "click-through" Agreement provided that the Issuer has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each EV Code Signing Object request, or a single Agreement MAY be used to cover multiple future EV Code Signing Object requests and the resulting objects, so long as each EV Code Signing Object that the Issuer issues to the Applicant is clearly covered by that Subscriber or Terms of Use Agreement.

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**: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures to 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. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of the Certificate**: An obligation and warranty to not knowingly sign software that contains Suspect Code and use the EV Code Signing Certificate as follows:
    a. only to sign code that complies with the requirements set forth in these Guidelines;
    b. solely in compliance with all applicable laws;
    c. solely for authorized company business; and
    d. solely in accordance with the Subscriber Agreement;
5. **Reporting and Revocation**: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in the event that:
    a. there is evidence that the certificate was used to sign suspect code;
    b. any information in the Certificate is, or becomes, incorrect or inaccurate; or
    c. there is any actual or suspected misuse or compromise of either the key activation data or the Subscriber's Private Key associated with the Public Key included in the Certificate;
6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance**: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Forum Guideline Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

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 a Subscriber or Terms of Use Agreement with its customer that contains the following obligations and warranties:

1. To use the EV Signature solely in compliance with the requirements set forth herein and the applicable EV Guidelines;
2. To use the EV Signature solely in compliance with all applicable laws;
3. To use the EV Signature solely for authorized company business;
4. To use the EV Signature solely in accordance with the Subscriber or Terms of Use Agreement;
5. To not knowingly submit software for signature that contains Suspect Code;
6. To inform the Signing Authority if it is discovered (by whatever means) that code submitted to the Signing Authority for signature contains malware or a serious vulnerability.

11 Verification Requirements

11.1 General Overview

This part of the Guidelines sets forth Verification Requirements and Acceptable Methods of Verification for each such Requirement**.**

11.1.1 Verification Requirements – Overview

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

(1) Verify Applicant's existence and identity, including;

(A) Verify the Applicant's legal existence and identity (as more fully set forth in Section 11.2 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.

An EV Timestamp Authority is NOT REQUIRED to validate in any way data submitted to it for time-stamping. It simply adds the time to the data that are presented to it, signs the result and appends its own certificate.

11.1.2 Acceptable Methods of Verification – Overview

As a general rule, the Issuer 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 Issuer is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

11.2 Verification of Applicant's Legal Existence and Identity

As specified in Section 11.2 of the EV Guidelines.

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

As specified in Section 11.3 of the EV Guidelines.

11.4 Verification of Applicant's Physical Existence

As specified in Section 11.4 of the EV Guidelines.

11.5 Verification of Applicant's Operational Existence

As specified in Section 11.5 of the EV Guidelines.

11.6 Verification of Applicant's Domain Name

Code Signing Certificates SHALL NOT include a Domain Name.

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

As specified in Section 11.7 of the EV Guidelines.

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

As specified in Section 11.8 of the EV Guidelines.

11.9 Verification of Approval of EV Code Signing Certificate Request

As specified in Section 11.9 of the EV Guidelines.

11.10 Verification of Certain Information Sources

As specified in Section 11.10 of the EV Guidelines.

11.11 Other Verification Requirements

As specified in Section 11119 of the EV Guidelines.

11.12 Final Cross-Correlation and Due Diligence

As specified in Section 11.12 of the EV Guidelines.

11.13 Requirements for Re-use of Existing Documentation

As specified in Section 11.13 of the EV Guidelines.

12 Certificate Issuance by a Root CA

Issuance of an EV Code Signing Object SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command to perform a certificate signing operation.

Root CA Private Keys MUST NOT be used to sign EV Code Signing Certificates or create EV Signatures.

13 Certificate Revocation and Status Checking

As specified in Section 13 of the EV Guidelines. In addition:

(A) Revocation Reasons: Subscribers are expected to not intentionally include Suspect Code in their signed software. Intentionally signing Suspect Code is a violation of the terms of the Subscriber Agreement, and will likely result in revocation of the EV Code Signing Object.

(B) Revocation Status Information: Certification Authorities are required to provide accurate and up-to-date revocation status information for at least one year following the expiration of the associated certificate. The CA SHALL, upon request, provide accurate and up-to-date revocation status information for a period not less than one year beyond expiry of the EV Code Signing Certificate.

(C) Revocation Processing: Whenever practical, platforms should check the revocation status of the certificates that they rely upon. However, this is not always practical. This situation occurs, for instance, when signed code has to be 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 EV 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.

(D) Revocation Consequences: 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.

(E) Responsiveness. The CA SHALL respond to all plausible notices that a signed software object containing Suspect Code verifies with a certificate that it has issued by setting the revocation status of that certificate to 'revoked'.

14 Employee and third party issues

14.1 Trustworthiness and Competence

Section 14.1 of the EV Guidelines applies to both CAs and Signing Authorities.

14.2 Delegation of Functions to Registration Authorities and Subcontractors

14.2.1 General

The CA MAY delegate the performance of all or any part of a requirement of these Guidelines to an Affiliate or a Registration Authority (RA) or subcontractor, provided that the process employed by the CA fulfills all of the requirements of Section 11.12. Affiliates and/or RAs must comply with the qualification requirements of Section 14.1 of these Guidelines.

The CA SHALL verify that the RA or subcontractor 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.

14.2.2 Enterprise RAs

The CA MAY NOT contractually authorize the Subject of a specified Valid EV Code Signing Certificate to perform the RA function and authorize the CA to issue additional EV Code Signing Certificates.

14.2.3 Guidelines Compliance Obligation

In all cases, the CA MUST contractually obligate each RA and subcontractor 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 Affiliate's, RA's, and subcontractor's compliance with these Requirements on an annual basis.

14.2.4 Allocation of Liability

As specified in Section 14.2.4 of the Baseline Requirements.

15 Data Records

Both CAs and Signing Authorities are required to abide by the obligations under Section 15 of the Baseline Requirements.

16 Data Security

The requirements of Section 16 of the Baseline Requirement apply to CAs and Signing Authorities. In addition, systems used to process and approve EV Code Signing Certificate and EV Signature requests MUST require actions by at least two trusted persons before creating an EV Code Signing Certificate or EV Signature.

In addition:

(1) An EV Timestamp Authority MUST protect its Private Key in a crypto module validated in accordance with FIPS 140-2 Level 2.

(2) An EV 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 FIPS 140-2 level 2 (or equivalent) crypto module. Techniques that may be used to satisfy this requirement include:

   a. Use of an HSM, verified by means of a manufacturer's certificate;

   b. A hardware crypto module provided by the CA;

   c. Contractual terms in the subscriber agreement requiring the Subscriber to protect the private key to a standard equivalent to FIPS 140-2 and with compliance being confirmed by means of an audit.

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

(4) CAs SHALL ensure that the Subscriber's private key is generated, stored and used in a crypto module that meets or exceeds the requirements of FIPS 140-2 level 2.Acceptable methods of satisfying this requirement include (but are not limited to) the following:

   a. The CA ships a suitable hardware crypto module, with a preinstalled key pair, in the form of a smartcard or USB device or similar;

   b. The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate indicating that the key is managed in a suitable hardware module;

   c. 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.

17 Audit

17.1 Eligible Audit Schemes

An Issuer issuing EV Code Signing Objects SHALL undergo an audit in accordance with one of the following schemes:

(i) WebTrust Program for CAs audit and WebTrust EV Program audit, or

(ii) ETSI TS 102 042 v2.1.1 audit.

If the Issuer is a Government Entity, an audit of the Issuer by the appropriate internal government auditing agency is acceptable in lieu of the audits specified above, provided that such internal government auditing agency publicly certifies in writing that its audit addresses the criteria specified in one of the above audit schemes and certifies that the government Issuer has successfully passed the audit.

EV audits MUST cover all Issuer obligations under these Guidelines regardless of whether they are performed directly by the Issuer, an RA, or subcontractor.

17.2 Audit Period

Issuers MUST undergo an annual audit that meets the criteria of Section 17.1.

17.3 Audit Record

Issuers SHOULD make its audit report publicly available no later than three months after the end of the audit period. If there is a delay greater than three months and if so requested by an Application Software Supplier, the Issuer MUST provide an explanatory letter signed by its auditor.

17.4 Pre-Issuance Readiness Audit

Issuers that are not already issuing EV Certificates must obtain a pre-issuance readiness audit under Section 17.4 of the EV Guidelines.

17.5 Regular Self Audits

Issuers must abide by the self audit requirements of the EV Guidelines. During the period in which it issues EV 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 EV Code Signing Certificates it has issued in the period beginning immediately after the last sample was taken. For all EV Code Signing Certificates where the Final Cross-Correlation and Due Diligence requirements of Section 11.12 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 EV Code Signing Certificates it has issued in the period beginning immediately after the last sample was taken.

17.6 Auditor Qualification

A Qualified Audit (as defined in Section 17.6 of the Baseline Requirements) MUST perform the Issuer's audit.

17.7 Root CA Key Pair Generation

As specified in Section 17.7 of the EV Guidelines.

18 Liability and Indemnification

Signing Authorities and CAs are both subject to the liability and indemnification obligations under Section 18 of the EV Guidelines.