Version 1.4.7~~6~~

CA/Browser Forum

Guidelines For The Issuance And Management Of Extended Validation Certificates

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

Guidelines for the Issuance and Management of Extended Validation Certificates

This version 1.4.7~~6~~ represents the Extended Validation Guidelines, as adopted by the CA/Browser Forum as of Ballot 122~~19~~, passed by the Forum on ~~24 March 2014~~ .

The Guidelines describe an integrated set of technologies, protocols, identity proofing, lifecycle management, and auditing practices specifying the minimum requirements that must be met in order to issue and maintain Extended Validation Certificates ("EV Certificates") concerning an organization. Subject Organization information from valid EV Certificates can then be used in a special manner by certain relying-party software applications (e.g., browser software) in order to provide users with a trustworthy confirmation of the identity of the entity that controls the Web site or other services they are accessing. Although initially intended for use in establishing Web-based data communication conduits via TLS/SSL protocols, extensions are envisioned for S/MIME, time-stamping, VoIP, IM, Web services, etc.

The primary purposes of Extended Validation Certificates are to: 1) identify the legal entity that controls a Web or service site, and 2) enable encrypted communications with that site. The secondary purposes include significantly enhancing cybersecurity by helping establish the legitimacy of an organization claiming to operate a Web site, and providing a vehicle that can be used to assist in addressing problems related to distributing malware, phishing, identity theft, and diverse forms of online fraud.

Notice to Readers

The Guidelines for the Issuance and Management of Extended Validation 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 Internet Web site commerce. 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.

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. Membership is listed in the Baseline Requirements.

Document History

Ver.	Ballot	Description	Adopted	Effective*
1.4.0	72	Reorganize EV Documents	29 May 2012	29 May 2012
1.4.1	75	NameConstraints Criticality Flag	8 June 2012	8 June 2012
1.4.2	101	EV 11.10.2 Accountants	31 May 2013	31 May 2013
1.4.3	104	Domain verification for EV Certificates	9 July 2013	9 July 2013
1.4.4	113	Revision to QIIS in EV Guidelines	13 Jan 2014	13 Jan 2014
1.4.5	114	Improvements to the EV Definitions	28 Jan 2014	28 Jan 2014
1.4.6	119	Remove "OfIncorporation" from OID descriptions in EVG 9.2.5	24 Mar 2014	24 Mar 2014
1.4.7	122	Verified Method of Communication in EVG 11.4.2		

Implementers' Note: Version 1.3 of these EV Guidelines was published on 20 November 2010 and supplemented through May 2012 when version 1.4 was published. ETSI TS 102 042 and ETSI TR 101 564 Technical Report: Guidance on ETSI TS 102 042 for Issuing Extended Validation Certificates for Auditors and CSPs reference these EV Guidelines. Version 1.4 of Webtrust® For Certification Authorities – Extended Validation Audit Criteria references version 1.4 of these EV Guidelines. The CA/Browser Forum continues to improve relevant guidelines, including this document, the Baseline Requirements, and the Network and Certificate System Security Requirements. We encourage all CAs to conform to each revision on the date specified without awaiting a corresponding update to an applicable audit criterion. In the event of a conflict between an existing audit criterion and a guideline revision, we will communicate with the audit community and attempt to resolve any uncertainty. We will respond to implementation questions directed to questions@cabforum.org. Our coordination with compliance auditors will continue as we develop guideline revision

cycles that harmonize with the revision cycles for audit criteria, the compliance auditing periods and cycles of CAs, and the CA/Browser Forum's guideline implementation dates.

Root Key Generation Script: A documented plan of procedures to be performed for the generation of the Root CA Key Pair**.**

Signing Authority: One or more Certificate Approvers designated to act on behalf of the Applicant.

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

Subsidiary Company: A company that is controlled by a Parent Company.

Superior Government Entity: Based on the structure of government in a political subdivision, the Government Entity or Entities that have the ability to manage, direct and control the activities of the Applicant.

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.

Translator: An individual or Business Entity that possesses the requisite knowledge and expertise to accurately translate the words of a document written in one language to the native language of the CA.

Verified Accountant Letter: A document meeting the requirements specified in Section 11.10.2 of these Guidelines

Verified Legal Opinion: A document meeting the requirements specified in Section 11.10.1 of these Guidelines.

Verified Method of Communication: The use of a public telecommunication routing number (ITU-T E.164-compliant fixed, mobile, fax, or SMS), an email address, or a postal delivery address, confirmed by the CA in accordance with Section 11.4.2 of the Guidelines as a reliable way of communicating with the Applicant.

WebTrust EV Program: The additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities.

WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

5 Abbreviations and Acronyms

Abbreviations and Acronyms are defined in the Baseline Requirements except as otherwise defined herein:

BIPM	International Bureau of Weights and Measures
BIS	(US Government) Bureau of Industry and Security
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPA	Chartered Professional Accountant
CSO	Chief Security Officer
EV	Extended Validation
gTLD	Generic Top-Level Domain
IFAC	International Federation of Accountants
IRS	Internal Revenue Service
ISP	Internet Service Provider
QGIS	Qualified Government Information Source
QTIS	Qualified Government Tax Information Source

business address for the Applicant, the CA MAY rely on the address in the QGIS to confirm the Applicant's or a Parent/Subsidiary Company's address as listed in the EV Certificate Request, and MAY rely on the Applicant's representation that such address is its Place of Business.

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

11.4.2 ~~Telephone Number for Applicant's Place of Business~~Verified Method of Communication

(1) Verification Requirements: To assist in communicating with the Applicant and confirming that the Applicant is aware of and approves issuance, the CA MUST establish at least one Verified Method of Communication with the Applicant~~ To further verify the Applicant's physical existence and business presence, as well as to assist in confirming other verification requirements, the CA MUST verify a main telephone number for one of the Applicant's Places of Business~~.

(2) Acceptable Methods of Verification: To verify ~~the~~a Verified Method of Communication with the Applicant~~'s telephone number~~, the CA MUST~~ perform items A and either B or C as listed below~~:

(A) Verify that the number or address belongs to the Applicant, or a Parent or Affiliate of the Applicant, by matching it with one of the Applicant's Places of Business in:

(i) records provided by the applicable phone company;

(ii) a QGIS, QTIS, or QIIS; or

(iii) a Verified Legal Opinion or Verified Accountant Letter; and

(B~~A~~) Confirm the ~~Applicant's telephone number~~ Verified Method of Communication by ~~calling~~ using it ~~and~~ to obtain~~ing~~ an affirmative response sufficient to enable a reasonable person to conclude that the Applicant, or a Parent of Affiliate of Applicant, ~~is reachable by telephone at the number dialed~~can be contacted reliably by using the Verified Method of Communication~~;~~

~~(B) Confirm that the telephone number is listed as one of the Applicant's or Parent/Subsidiary Company's or Principal Individual's (for business entities) telephone numbers, matching an address of one of the Applicant's Places of Business in records provided by the applicable phone company, or, alternatively, in at least one QIIS, QGIS, or QTIS;~~

~~(C) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant's telephone number, as provided, is a main phone number for the Applicant's Place of Business~~.

11.5 Verification of Applicant's Operational Existence

11.5.1 Verification Requirements

If the Applicant, or a Parent or Affiliate of the Applicant, has been in existence for less than three years, as indicated by the records of the Incorporating Agency or Registration Agency, and is not listed in either the current version of one QIIS or QTIS, the CA MUST verify that the Applicant has the ability to engage in business. In other words, if the Applicant is a Subsidiary or Affiliate of an entity that the CA verified as in existence for three or more years, then the CA MAY rely on the existence of the Parent or Affiliate as verification of the Applicant's operational existence.

11.5.2 Acceptable Methods of Verification

To verify the Applicant's operational existence, the CA MUST perform one of the following:

(1) Verify that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution. The CA MUST receive authenticated documentation directly from a Regulated Financial Institution verifying that the Applicant has an active current Demand Deposit Account with the institution.

(2) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in Section 14.1 of these Guidelines. When employees under the control of the CA do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA MAY:

(A) Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or

(B) When the CA has utilized the services of an RA, the CA MAY rely on the language skills of the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with Section 11.12, Subsections (1), (2) and (3). Notwithstanding the foregoing, prior to issuing the EV Certificate, the CA MUST review the work completed by the RA and determine that all requirements have been met; or

(C) When the CA has utilized the services of an RA, the CA MAY rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with this section and is subjected to the Audit Requirements of Sections 17.5 and 17.6.

In the case of Enterprise EV Certificates to be issued in compliance with the requirements of Section 14.2 of these Guidelines, the Enterprise RA MAY perform the requirements of this Final Cross-Correlation and Due Diligence section.

11.13 Requirements for Re-use of Existing Documentation

11.13.1 For Validated Data

(1) The age of validated data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:

(A) Legal existence and identity – thirteen months;

(B) Assumed name – thirteen months;

(C) Address of Place of Business – thirteen months, but thereafter data MAY be refreshed by checking a Qualified Independent Information Source, even where a site visit was originally required;

(D) ~~Telephone number for Place of Business~~ Verified Method of Communication – thirteen months;

(E) Bank account verification – thirteen months;

(F) Domain Name – thirteen months;

(G) Identity and authority of Certificate Approver – thirteen months, unless a contract is in place between the CA and the Applicant that specifies a different term, in which case, the term specified in such contract will control. For example, the contract MAY use terms that allow the assignment of roles that are perpetual until revoked, or until the contract expires or is terminated.

(2) The age of information used by the CA to verify such an EV Certificate Request MUST NOT exceed the Maximum Validity Period for such information set forth above in subsection (1), based on the date the information was last updated by the QIIS, QGIS, or QTIS (e.g., if an online database was accessed by the CA on July 1, but contained data last updated by the QIIS, QGIS, or QTIS on February 1 of the same year, then the date on which the information was obtained would be considered to be February 1).

(3) The CA MAY issue multiple EV Certificates listing the same Subject and based on a single EV Certificate Request, subject to the aging and updating requirement stated above.

(4) Each EV Certificate issued by the CA MUST be supported by a valid current EV Certificate Request and a Subscriber Agreement signed by the appropriate Applicant Representative on behalf of the Applicant or Terms of Use acknowledged by the appropriate Applicant Representative.

(5) In the case of outdated information, the CA MUST repeat the verification processes required in these Guidelines.

11.13.2 Validation for Existing Subscribers

In conjunction with an EV Certificate Request placed by an Applicant who is already a customer of the CA, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the EV Certificate will still be accurate and valid.

11.13.3 Exceptions

Notwithstanding the requirements set forth in Section 11.13.1, when performing the authentication and verification tasks for issuing an EV Certificate where the Applicant has a current valid EV Certificate issued by the CA, a CA MAY:

(1) Rely on its prior authentication and verification of:

(A) The Principal Individual of a Business Entity under Section 11.2.2 (4) if the Principal Individual is the same as the Principal Individual verified by the CA in connection with the previously issued EV Certificate;

(B) The Applicant's Place of Business under Section 11.4.1;

(C) The ~~telephone number of the Applicant's Place of Business~~ Verified Method of Communication required by Section 11.4.2, but still MUST perform the verification required by Section 11.4.2 (2)(~~A~~B);

(D) The Applicant's Operational Existence under Section 11.5;

(E) The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester under Section 11.7, except where a contract is in place between the CA and the Applicant that specifies a specific term for the authority of the Contract Signer, and/or the Certificate Approver, and/or Certificate Requester in which case, the term specified in such contract will control;

(F) The email address used by the CA for independent confirmation from the Applicant under Section 11.10.4 (1)(B)(ii);

(2) Rely on a prior Verified Legal Opinion or Accountant Letter that established:

(A) The Applicant's right to use the specified Domain Name under Section 11.6, provided that the CA verifies that either:

(i) The WHOIS record still shows the same registrant as indicated when the CA received the prior Verified Legal Opinion or Verified Accountant Letter, or

(ii) The Applicant establishes domain control via a process permitted under Section 11.6.

11.13.4 Validation of Re-issuance Requests

A CA may rely on previously verified information to issue a replacement certificate where:

(1) The expiration date of the replacement certificate is the same as the expiration date of the currently valid EV Certificate that is being replaced, and

(2) The Subject of the Certificate is the same as the Subject in the currently valid EV Certificate that is being replaced.

12 Certificate Issuance by a Root CA

Certificate issuance by the Root CA 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 in order for the Root CA to perform a certificate signing operation.

Root CA Private Keys MUST NOT be used to sign EV Certificates.

13 Certificate Revocation and Status Checking

The requirements in Section 13 of the Baseline Requirements apply equally to EV Certificates. However, CAs MUST ensure that CRLs for an EV Certificate chain can be downloaded in no more than three (3) seconds over an analog telephone line under normal network conditions.