

CA/Browser Forum

Guidelines For The Issuance And Management Of Extended Validation Certificates

Copyright © 2007-2017, The CA/Browser Forum. This work is licensed under a Creative Commons Attribution 4.0 International license.

Verbatim copying and distribution of this entire document is permitted in any medium without royalty, provided this notice is preserved.

Upon request, the CA / Browser Forum may grant permission to make a translation of these guidelines into a language other than English. In such circumstance, copyright in the translation remains with the CA / Browser Forum. In the event that a discrepancy arises between interpretations of a translated version and the original English version, the original English version shall govern. A translated version of the guidelines must prominently display the following statement in the language of the translation:-

'Copyright © 2007-2017 The CA/Browser Forum. This work is licensed under a Creative Commons Attribution 4.0 International license.

This document is a translation of the original English version. In the event that a discrepancy arises between interpretations of this version and the original English version, the original English version shall govern.'

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 1.6.19 represents the Extended Validation Guidelines, as adopted by the CA/Browser Forum as of Ballot ~~171~~180, passed by the Forum on ~~17 January~~ 20176.

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 at <https://cabforum.org/members/>.

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	120	Affiliate Authority to Verify Domain	5 June 2014	5 June 2014
1.4.8	124	Business Entity Clarification	5 June 2014	5 June 2014
1.4.9	127	Verification of Name, Title and Agency	17 July 2014	17 July 2014
1.5.0	126	Operational Existence	24 July 2014	24 July 2014
1.5.1	131	Verified Method of Communication	12 Sept 2014	12 Sept 2014
1.5.2	123	Reuse of Information	16 Oct. 2014	16 Oct. 2014
1.5.3	144	Validation rules for .onion names	18 Feb. 2015	18 Feb. 2015
1.5.4	146	Convert Baseline Requirements to RFC 3647 Framework	16 Apr. 2015	16 Apr. 2015
1.5.5	145	Operational Existence for Government Entities	5 Mar. 2015	5 Mar. 2015
1.5.6	147	Attorney-Accountant Letter Changes	25 June 2015	25 June 2015
1.5.7	151	Addition of Optional OIDs for Indicating Level of Validation	28 Sept 2015	28 Sept 2015
1.5.8	162	Sunset of Exceptions	15 Mar. 2016	15 Mar. 2016
1.5.9	163	Fix Errata in EV Guidelines 11.2.1	18 Mar. 2016	18 Mar. 2016
1.6.0	171	Updating ETSI Standards in CABF documents	1 July 2016	1 July 2016
1.6.1	180	In EV 11.7.1, removed outdated cross-reference to BR 3.2.2.4(7)	7 Jan. 2017	7 Jan. 2017

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 version 1.3 of these EV Guidelines, and ETSI Draft EN 319 411-1 references version 1.4. Version 1.4.5 of Webtrust® For Certification Authorities – Extended Validation Audit Criteria references version 1.4.5 of these EV Guidelines. As illustrated in the Document History table above, the CA/Browser Forum continues to improve relevant industry 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.

11.7. Verification of Applicant's Domain Name

11.7.1. Verification Requirements

- (1) For each Fully-Qualified Domain Name listed in a Certificate, other than a Domain Name with .onion in the right-most label of the Domain Name, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as "Applicant" for the purposes of this section) either is the Domain Name Registrant or has control over the FQDN using a procedure specified in Section 3.2.2.4 of the Baseline Requirements, ~~except that a CA MAY NOT verify a domain using the procedure described subsection 3.2.2.4(7)~~. For a Certificate issued to a Domain Name with .onion in the right-most label of the Domain Name, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant's control over the .onion Domain Name in accordance with Appendix F.
- (2) **Mixed Character Set Domain Names:** EV Certificates MAY include Domain Names containing mixed character sets only in compliance with the rules set forth by the domain registrar. The CA MUST visually compare any Domain Names with mixed character sets with known high risk domains. If a similarity is found, then the EV Certificate Request MUST be flagged as High Risk. The CA must perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

11.8. Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

11.8.1. Verification Requirements

For both the Contract Signer and the Certificate Approver, the CA MUST verify the following.

- (1) **Name, Title and Agency:** The CA MUST verify the name and title of the Contract Signer and the Certificate Approver, as applicable. The CA MUST also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.
- (2) **Signing Authority of Contract Signer:** The CA MUST verify that the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.
- (3) **EV Authority of Certificate Approver:** The CA MUST verify, through a source other than the Certificate Approver him- or herself, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request:
 - (A) Submit, and, if applicable, authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and
 - (B) Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV Certificate; and
 - (C) Approve EV Certificate Requests submitted by a Certificate Requester.

11.8.2. Acceptable Methods of Verification – Name, Title and Agency

Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include the following.

- (1) **Name and Title:** The CA MAY verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable assurance that a person claiming to act in such a role is in fact the named person designated to act in such role.
- (2) **Agency:** The CA MAY verify the agency of the Contract Signer and the Certificate Approver by: