# WebTrust SM/TM for Certification Authorities

# WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5

**Based on:**

## *CA/Browser Forum*

## *Guidelines for the Issuance and Management of Extended Validation SSL Certificates –* *Version 1.4.5*

## RELEASE DATE

April 3, 2014

## EFFECTIVE DATE

April 3, 2014

# TABLE OF CONTENTS



This document has been prepared for the use by those auditors recognized as eligible to perform EV audits by the CA/Browser Forum, Certification Authorities, Browsers and users of Extended Validation Certificates.

This document was prepared by the WebTrust for Certification Authorities Task Force. Members of this Group are:

| **Chair** | **Staff Contact** |
|---|---|
| Donald E. Sheehy<br>*Deloitte LLP*<br><br>David Roque<br>*Ernst & Young LLP*<br><br>Reema Anand<br>*KPMG LLP*<br><br>Jeffrey Ward<br>*Stone Carlie & Company LLC* | Bryan Walker<br>*CPA Canada* |

The Task Force would like to express its appreciation for the contributions of Mark Lundin and Michael Greene who were members of the Task Force since its inception until August 1, 2012 and June 30, 2013 respectively. The Task Force would also like to thank Robert Ikeoka, KPMG LLP, Donoghue Clarke, Ernst & Young LLP, and Daniel J. Adam, Deloitte LLP, for their efforts in the preparation of this guide.

# INTRODUCTION

The growth of internet transactions has emphasized the importance of strong authentication of the identity of web sites, domain owners and online servers. The Certificate Authorities ("CA") and browser developers have worked together to develop guidelines that create the basis for differentiating certificates which have stronger authentication standards than other certificates. Certificates that have been issued under stronger authentication controls, processes and procedures are called Extended Validation Certificates ("EV Certificates"). EV Certificates are currently differentiated by their intended use as:

- Certificates intended to ensure the identity of a remote computer ("EV SSL Certificates"); and
- Certificates intended to ensure the identity of a software publisher and the integrity of software code ("EV Code Signing Certificates").

This document addresses EV SSL Certificates.

A working group known as the CA/Browser Forum ("CA/B Forum" or the "Forum") consisting of many of the issuers of digital certificates and browser developers has created a set of guidelines that set out the expected requirements for issuing EV SSL Certificates. The guidelines entitled "Guidelines for the Issuance and Management of Extended Validation SSL Certificates" ("EV SSL Guidelines") can be found at http://www.cabforum.org/.

CAs and browser developers have recognized the importance of an independent third party audit[1] of the controls, processes and procedures of CAs. Accordingly, the EV SSL Guidelines include a specific requirement for CAs that wish to issue EV SSL certificates.

The purpose of these WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL ("EV SSL Criteria") is to set criteria that would be used as a basis for an auditor to conduct an EV SSL audit.

***Adoption***

Version 1.4.5 of the CA/Browser Forum EV SSL Guidelines became effective on 28 January 2014. These EV SSL Criteria become applicable upon release.

***Navigating Baseline Requirements in an EV SSL audit***

In 2011, the Forum released its Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") Version 1.0 with an effective date of 1 July 2012. Since the issuance of Version 1.0, a number of updates have been made, with the latest edition being Version 1.1.6 that became effective 29 July 2013. The EV SSL Guidelines, and these EV SSL Criteria, at times makes reference to the Baseline Requirements, and many guidelines which used to be previously detailed in the EV SSL Guidelines are now incorporated by reference to the Baseline Requirements. To facilitate the EV SSL Audit, however, these requirements continued to be detailed in these EV SSL Criteria. These criteria incorporate and make reference to Version 1.1.6 of the Baseline Requirements.

***Errata***

The CA/Browser Forum may periodically publish errata that capture changes to the EV SSL Guidelines. In addition, the CA/Browser Forum will periodically modify the EV SSL Guidelines to reflect more substantive changes in a point version (e.g., version 1.5). The auditor would need to consider only the updated approved

[1] For the purposes of this document, the term "audit" has been used to describe an assurance engagement in which an auditor (practitioner) expresses a conclusion designed to enhance the degree of confidence on the intended users about the outcome of the evaluation against criteria. This is referred to as an "examination" in some jurisdictions.

version. The auditor is not required to consider the errata document.

The EV SSL Criteria requires a current audit of the Certification Authority as required by the CA/Browser Forum Guidelines such as the WebTrust for CAs audit or ETSI TS102 042 v2.1.1. The two audits would normally be conducted simultaneously. For CAs that have successfully (successfully meaning an opinion without reservation issued by an auditor) undergone a WebTrust for CA audit or ETSI TS102 042 v2.1.1 and the report is still current the procedures undertaken by the auditor would only be those that are necessary to examine the added criteria for EV SSL certificates. The currently valid Certification Authorities audit would not need to be updated to a more recent date that would match the date of the EV audit.

If the CA does not have a currently valid WebTrust Seal of Assurance for CAs or an ETSI TS 102 042 audit, then before issuing EV SSL Certificates, the CA and its Root CA must successfully complete either:

i. A point-in-time audit against the WebTrust for CA program (based on the WebTrust Principles and Criteria for Certification Authorities), AND a point-in-time audit against these EV SSL Criteria; OR

ii. An ETSI TS 102 042 v2.1.1 audit.

# WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL

**PRINCIPLE 1**: **Certification Authority Extended Validation SSL Business Practices Disclosure** - The Certification Authority (CA) discloses its Extended Validation (EV) SSL Certificate practices and procedures and its commitment to provide EV SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines.

| | |
|---|---|
| 1 | The CA discloses[2] on its website its:<br>Ï EV SSL Certificate practices, policies and procedures,<br>Ï CAs in the hierarchy whose subject name is the same as the EV SSL issuing CA, and<br>Ï its commitment to conform to CA/Browser Forum Guidelines for Extended Validation Certificates.<br>(See EV SSL Guidelines Section 8.2.2 ) |
| 2 | The Certificate Authority has published guidelines for revoking EV SSL Certificates.<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.1.1 ) |
| 3 | The CA provides instructions to Subscribers, Relying Parties, Application Software Vendors and other third parties for reporting complaints or suspected private key compromise, EV SSL Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV SSL Certificates to the CA.<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.1.2) |
| 4 | The CA maintains controls to provide reasonable assurance that there is public access to the CPS on a 24x7 basis, and the CPS is structured in accordance with either RFC 2527 or RFC 3647.<br>(See EV SSL Guidelines Section 8.2.2) |

[2] The criteria are those that are to be tested for the purpose of expressing an opinion on these EV SSL Criteria. For an initial "readiness assessment" where there has not been a minimum of two months of operations disclosure to the public is not required. The CA, however, must have all other aspects of the disclosure completed such that the only action remaining is to activate the disclosure so that it can be accessed by users in accordance with the EV SSL Guidelines.

**PRINCIPLE 2: Service Integrity -** The Certification Authority maintains effective controls to provide reasonable assurance that:

- Ï EV SSL Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
- Ï The integrity of keys and EV SSL certificates it manages is established and protected throughout their life cycles.

| | |
|---|---|
| | The following criteria apply to both new and renewed EV SSL Certificates. |
| | **Subscriber Profile** |
| 1 | The CA maintains controls to provide reasonable assurance that it issues EV SSL Certificates to Private Organizations, Government Entities, and Business Entities as defined within the EV SSL Guidelines that meet the following requirements:<br>For Private Organizations<br>• the organization is a legally recognized entity whose existence was created or recognized by a by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation registration number, etc.) or created or recognized by a Government Agency (e.g. under a charter, treaty, convention, or equivalent recognition instrument);;<br>• the entity designated with the Incorporating or Registration Agency a Registered Agent, or a Registered Office (as required under the laws of the jurisdiction of Incorporation or Registration), or an equivalent facility;<br>• the entity is not designated as inactive, invalid, non-current or equivalent in records of the Incorporating Agency or Registration Agency;<br>• the entity has a verifiable physical existence and business presence;<br>• the entity's Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business is not in a country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and<br>• the entity is not listed on a published government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.<br>(See EV SSL Guidelines Section 8.5.2)<br>OR<br>For Government Entities<br>• the entity's legal existence was established by the political subdivision in which the entity operates;<br>• the entity is not in a country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and<br>• the entity is not listed on a government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.<br>(See EV SSL Guidelines Section 8.5.3)<br>OR |

| | |
|---|---|
| | For Business Entities<br>• the entity is a legally recognized entity that filed certain forms with a Registration Agency in its Jurisdiction, the Registration Agency issued or approved the entity's charter, certificate, or license, and the entity's existence can be verified with that Registration Agency;<br>• the entity has a verifiable physical existence and business presence;<br>• at least one Principal Individual associated with the entity(owners, partners, managing members, directors or officers) is identified and validated by the CA;<br>• the identified Principal Individual (owners, partners, managing members, directors or officers) attests to the representations made in the Subscriber agreement;<br>• the CA verifies the entity's use of any assumed name, used to represent the entity pursuant to the requirements of Section 11.3;<br>• the entity and the identified Principal Individual (owners, partners, managing members, directors or officers) associated with the entity are not located in a country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and<br>• the entity and the identified Principal Individual (owners, partners, managing members, directors or officers) associated with the entity are not listed on any published government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.<br>(See EV SSL Guidelines Section 8.5.4)<br>OR<br>For Non-commercial enterprises (International Organization Entities)<br>• the Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government and<br>• the Applicant is not headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and<br>• the Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.<br>(See EV SSL Guidelines Section 8.5.5) |
| | **EV SSL CERTIFICATE CONTENT AND PROFILE** |
| 2 | The CA maintains controls to provide reasonable assurance that the EV SSL certificates issued meet the minimum requirements for Certificate Content and profile, including additional technical requirements as specifically established in section 9 of the EV SSL Guidelines including the following:<br>• Issuer Common Name Field<br>• Issuer Domain Component Field<br>• Issuer Organization Name Field<br>• Issuer Country Name Field<br>• full legal organization name and if space is available the d/b/a name may also be disclosed<br>• Subject Alternative Name Extension<br>• Subject Common Name Field<br>• Subject Business Category Field<br>• Subject Jurisdiction of Incorporation or Registration Field<br>• Subject Registration Number Field |

| | |
|---|---|
| | • Subject Physical Address of Place of Business Field<br>• Other Subject Attributes<br>(See EV SSL Guidelines Section 9 including Section 9.1 that refers to Baseline Requirements Section 9.1) |
| 3 | The CA maintains controls and procedures to provide reasonable assurance that the EV SSL Certificates issued include the minimum requirements for the content of EV SSL Certificates as established in the EV SSL Guidelines relating to:<br>• EV Subscriber Certificates<br>• EV Subordinate CA Certificates.<br>(See EV SSL Guidelines Section 9.3.2, 9.3.4 and 9.3.5) |
| 4 | For EV SSL Certificates issued to Subordinate CAs, the CA maintains controls and procedures to provide reasonable assurance that the certificates contain one or more OID that explicitly defines the EV Policies that Subordinate CA supports.<br>(See EV SSL Guidelines Section 9.3.4) |
| 5 | The CA maintains controls and procedures to provide reasonable assurance that EV SSL Certificates are valid for a period not exceeding 27 months.<br>(See EV SSL Guidelines Section 9.4) |
| 6 | The CA maintains controls and procedures to provide reasonable assurance that the data that supports the EV SSL Certificates is revalidated within the timeframes established in the EV SSL Guidelines.<br>(See EV SSL Guidelines Section 11.13) |
| | **EV SSL CERTIFICATE REQUEST REQUIREMENTS** |
| 7 | The CA maintains controls and procedures to provide reasonable assurance that the EV SSL Certificate Request is:<br>• obtained and complete prior to the issuance of EV SSL Certificates (See EV SSL Guidelines Section 10),<br>• signed by an authorized individual (Certificate Requester),<br>• approved by an authorized individual (Certificate Approver)<br>• properly certified as to being true and correct by the applicant, and<br>• contains the information specified in Section 10 of the EV SSL Guidelines. |
| | **Subscriber Agreement and Terms of Use** |
| 8 | The CA maintains controls and procedures to provide reasonable assurance that Subscriber Agreements: |

| | |
|---|---|
| | • are signed by an authorized Contract Signer,<br>• names the applicant and the individual Contract Signer, and<br>• contains provisions imposing obligations and warranties on the Application relating to<br>  ○ the accuracy of information<br>  ○ protection of Private Key<br>  ○ acceptance of EV SSL Certificate<br>  ○ use of EV SSL Certificate<br>  ○ reporting and revocation upon compromise<br>  ○ termination of use of EV SSL Certificate.<br>  ○ responsiveness<br>  ○ acknowledgement and acceptance<br>(See EV SSL Guidelines Section 10.3 that refers to Baseline Requirements Section 10.3) |
| | **INFORMATION VERIFICATION REQUIREMENTS** |
| | **Verification of Applicant's Legal Existence and Identity** |
| 9 | The CA maintains controls and procedures to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the EV SSL Guidelines:<br>Private Organization Subjects<br>• legal Existence and Identity<br>• legal Existence and Identity – Assumed Name<br>• organization Name<br>• registration Number<br>• registered agent<br>• relationship to the Parent, Subsidiary, or Affiliate (if applicable)<br>Government Entity<br>• legal Existence<br>• entity Name<br>• registration Number<br>Business Entity<br>• legal Existence<br>• organization Name<br>• registration Number<br>• principal Individual.<br>• relationship to the Parent, Subsidiary, or Affiliate (if applicable)<br>Non-Commercial Entity<br>• International Organization Entities<br>  ○ legal entities<br>  ○ entity name |

| | |
|---|---|
| | ○ registration number.<br>(See EV SSL Guidelines Sections 11.1, 11.2,11.3, and 11.11.3) |
| | **Verification of Applicant** |
| 10 | The CA maintains controls and procedures to provide reasonable assurance that it verifies the physical address provided by Applicant is an address where Applicant or a Parent /Subsidiary company conducts business operations (e.g., not a mail drop or P.O. box, or 'care of' C/O address, such as an address of an agent of the Organization), and is the address of Applicant's Place of Business using a method of verification established by the EV SSL Guidelines.<br>(See EV SSL Guidelines Section 11.4.1) |
| 11 | The CA maintains controls and procedures to provide reasonable assurance that the telephone number provided by the Applicant is verified as a main phone number for Applicant's Place of Business by performing the steps set out in the EV SSL Guidelines.<br>(See EV SSL Guidelines Section 11.4.2) |
| 12 | If the Applicant, has been in existence for less than three (3) years, as indicated by the records of the Incorporating Agency or Registration Agency, and is not listed in either the current version of one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source, and is not a Subsidiary or Affiliate of an entity that the CA verified as in existence for three or more years, the CA maintains controls to provide reasonable assurance that the Applicant is actively engaged in business by:<br>• verifying that the Applicant has an active current Demand Deposit Account with a regulated financial institution, or<br>• obtaining a Verified Legal Opinion or a Verified Accountant Letter that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.<br>(See EV SSL Guidelines Section 11.5) |
| 13 | The CA maintains controls and procedures to provide reasonable assurance that for each Fully-Qualified Domain Name listed in a Certificate, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by only using at least one of the following verification methods:<br>1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;<br>2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;<br>3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;<br>4. Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; |

| | |
|---|---|
| | 5. Relying upon a Domain Authorization Document; or<br>6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN.<br>(See EV SSL Guidelines Section 11.6.1 that refers to Baseline Requirements Section 11.1.1) |
| | **Verification of Other** |
| 14 | The CA maintains controls to provide reasonable assurance that it identifies "High Risk Applicants" and undertakes additional precautions as are reasonably necessary to ensure that such Applicants are properly verified using a verification method below:<br>• the CA may identify high risk requests by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and by automatically flagging certificate requests that match these lists for further scrutiny before issuance.<br>• the CA uses information identified by the CA's high-risk criteria to flag suspicious certificate requests. The CA follows a documented procedure for performing additional verification of any certificate request flagged as suspicious or high risk.<br>(See EV SSL Guidelines Section 11.11.1 that refers to Baseline Requirements Section 11.5) |
| 15 | The CA maintains controls to provide reasonable assurance that no EV SSL Certificate is issued if the Applicant, the Contract Signer, the Certificate Approver or the Applicant's Jurisdiction of Incorporation, Registration, or place of Business is:<br>• on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or<br>• has its Jurisdiction of Incorporation, or Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business.<br>(See EV SSL Guidelines Section 11.11.2) |
| | **Verification of Contract Signer and Approver** |
| 16 | The CA maintains controls and procedures to provide reasonable assurance that it verifies, using a method of verification established by the EV SSL Guidelines:<br>• the name and title of the Contract Signer and the Certificate Approver, as applicable and verifying that the Contract Signer and the Certificate Approver are agents representing the Applicant;<br>• through a source other than the Contract Signer, that the Contract Signer is expressly 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 Applicant ("Signing Authority");<br>• through a source other than the Certificate Approver, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV SSL Certificate Request ("EV Authority") to: |

| | |
|---|---|
| | ○ submit, and if applicable authorize a Certificate Requester to submit, the EV SSL Certificate Request on behalf of the Applicant; and<br>○ provide, and if applicable authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV SSL Certificate; and<br>○ approve EV SSL Certificate Requests submitted by a Certificate Requester.<br>(See EV SSL Guidelines Section 11.7) |
| | **Verification of EV SSL Certificate Requests** |
| 17 | The CA maintains controls to provide reasonable assurance, using a method of verification established in the EV SSL Guidelines that:<br>• subscriber Agreements are signed by an authorized Contract signer;<br>• the EV SSL Certificate Request is signed by the Certificate Requester submitting the document<br>• if the Certificate requester is not also an authorized Certificate Approver, an authorized Certificate Approver independently approves the EV SSL Certificate Request unless pre-authorized; and<br>• signatures have been properly authenticated.<br>(See EV SSL Guidelines Section 11.8 and 11.9) |
| 18 | In cases where an EV SSL Certificate Request is submitted by a Certificate Requester, the CA maintains controls to provide reasonable assurance that, before it issues the requested EV SSL Certificate, it verifies that an authorized Certificate Approver reviewed and approved the EV SSL Certificate Request.<br>(See EV SSL Guidelines Section 11.9) |
| 19 | The CA maintains controls to provide reasonable assurance that it verifies information sources prior to placing reliance on them using a verification procedure set out in the EV SSL Guidelines. The verification includes:<br>• with respect to legal opinions;<br>○ the independent status of the author,<br>○ the basis of the opinion, and<br>○ authenticity.<br>• with respect to accountants letters;<br>○ the status of the author,<br>○ the basis of the opinion, and<br>○ authenticity.<br>• with respect to face-to-face vetting documents;<br>○ qualification of third-party validator,<br>○ document chain of custody, and<br>○ verification of attestation.<br>• with respect to independent confirmation from applicant;<br>○ the request is initiated by the CA requesting verification of particular facts,<br>○ the request is directed to a Confirming Person at the Applicant or at the Applicant's Registered Agent or Registered Office using one of the acceptable methods stated by the CA/Browser Forum.<br>○ the Confirming Person confirms the fact or issue. |

| | |
|---|---|
| | • with respect to Qualified Independent Information Sources (QIIS)<br>  o the database used is a QIIS as defined by the EV SSL Guidelines 11.10.5).<br>• with respect to Qualified Government Information Sources (QGIS)<br>  o the database used is a QGIS as defined by the EV SSL Guidelines 11.10.6.<br>• with respect to Qualified Government Tax Information Source (QGTIS)<br>  o a Qualified Governmental information source is used that specifically contains tax information relating to Private Organizations, Business Entities or Individuals as defined by the EV SSL Guidelines 11.10.7.<br>(See EV SSL Guidelines Section 11.10 and for Certificate Renewals Section 11.13) |
| | **Validation for Existing Subscribers (previously EV Certificate Renewal Verification Requirements)** |
| 20 | In conjunction with an EV SSL Certificate Request placed by an Applicant who is already a customer of the CA, the CA performs 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 SSL Certificate will still be accurate and valid.<br>(See EV SSL Guidelines Section 11.13) |
| | **Other Matters** |
| 21 | Except for certificate requests approved by an Enterprise Registration Authority ("RA"), the CA maintains controls to provide reasonable assurance that:<br>• the set of information gathered to support a certificate request is reviewed for completeness and accuracy by an individual who did not gather such information;<br>• any identified discrepancies are documented and resolved before certificate issuance; and<br>• in the case where some or all of the documentation used to support the application is in a language other than the CA's normal operating language, the Final Cross-Correlation and Due Diligence is performed by employees under its control having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained (See Section 29 of the EV SSL Guidelines). When employees do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA may:<br>  o rely on the translations by a Translator or, if an RA is used, the CA reviews the work completed by the RA and determine that all requirements have been met; and<br>  o The CA may rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with Section 24 and is subjected to the Audit Requirements of Sections 14.1.2 and 14.1.3 as specified in the EV SSL Guidelines.<br>(See EV SSL Guidelines Section 11.12, 14.1.3, 17) |
| 22 | The CA maintains controls to provide reasonable assurance that it verifies that the Delegated Third Party, involved in the issuance of EV SSL Certificates, meet training, skills, document retention, and event logging requirements.<br>(See EV SSL Guidelines Section 14.2.1) |

| | |
|---|---|
| 23 | The CA maintains controls to provide reasonable assurance that RAs, subcontractors, and Enterprise RAs are contractually obligated to comply with the applicable requirements in the EV SSL Guidelines and to perform them as required of the CA itself.<br><br>(See EV SSL Guidelines Section 14.2) |
| | **CERTIFICATE STATUS CHECKING AND REVOCATION** |
| 24 | The CA maintains controls to provide reasonable assurance that the CA includes revocation information for Subordinate Certificates and Subscriber Certificates in accordance with Appendix B of the Baseline Requirements.<br><br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.2.1) |
| 25 | If the Subscriber Certificate is for a high-traffic FQDN, the CA may rely on stapling, in accordance with [RFC4366], to distribute its OCSP responses. If the CA relies on stapling the CA maintains controls to provide reasonable assurance that:<br><br>• the Subscriber "staples" the OCSP response for the Certificate in its TLS handshake, and<br>• this requirement is enforced on the Subscriber either contractually, through the Subscriber or Terms of Use Agreement, or by technical review measures implement by the CA.<br><br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.2.1) |
| 26 | The CA maintains controls to provide reasonable assurance that a repository is available 24x7 that enable Internet browsers to check online the current status of all unexpired certificates.<br><br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.2.2) |
| 27 | The CA maintains controls to provide reasonable assurance that:<br><br>• for EV SSL Certificates or Subordinate CA Certificates issued to entities not controlled by the entity that controls the Root CA<br>  o CRLs are updated and reissued at least every seven (7) days, and the nextUpdate field value is not more than ten (10) days, or<br>  o if the CA provides revocation of information via an Online Certificate Status Protocol (OCSP) service, the OCSP service is updated at least every four (4) days, and OCSP responses from this service have a maximum expiration time of ten (10) days.<br>• for subordinate CA Certificates controlled by the Root CA<br>  o CRLs are updated and reissued at least every twelve (12) months, and (ii) within 24 hours if a Subordinate CA Certificate is revoked, and the nextUpdate field value is not more than twelve (12) months; or<br>  o if the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, the OCSP service is updated at least every twelve (12) months, and within 24 hours if a Subordinate CA certificate is revoked, and the OCSP responses from this service have a maximum expiration time of twelve (12) months.<br><br>The CA maintains controls to provide reasonable assurance that the CA supports an OCSP capability using the GET method for Certificates issued in accordance with these Requirements. (**Effective January** |

| | |
|---|---|
| | **1, 2013**).<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.2.2) |
| 28 | For CA that operate only a CRL capability, the CA maintains controls to provide reasonable assurance that an EV SSL certificate chain can be downloaded in no more than 3 seconds over an analogue telephone line under normal network conditions.<br>(See EV SSL Guidelines Section 13) |
| 29 | The CA maintains controls to provide reasonable assurance that the CA can operate and maintain its CRL and OCSP capability to provide a response time of ten seconds or less under normal operating conditions.<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.2.3) |
| 30 | The CA maintains controls to provide reasonable assurance that Revocation entries on a CRL or OCSP are not removed until after the expiration date of the revoked EV SSL Certificate.<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.2.4) |
| 31 | The CA maintains controls to provide reasonable assurance that the OCSP responses conforms to RFC2560 and/or RFC5019. The OCSP responses either:<br>• Be signed by the CA that issued the Certificates whose revocation status is being checked, or<br>• Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. If so, the OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC2560<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.2.5) |
| 32 | The CA maintains controls to provide reasonable assurance that OCSP responders do not respond with a "good" status for non-issued certificates. (As of the effective date set by the CA/B Forum)<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.2.6) |
| 33 | The CA maintains controls to provide reasonable assurance that the CA:<br>• provides a process for Subscribers to request revocation of their own Certificates.<br>• describes the process in the CA's Certificate Policy or Certification Practice Statement.<br>• maintains a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.1.1) |
| 34 | The CA maintains controls to provide reasonable assurance that the CA provides Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates and publicly discloses the instructions through a readily accessible online means. |

| | |
|---|---|
| | (See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.1.2) |
| 35 | The CA maintains controls to provide reasonable assurance that the CA begins investigation of a Certificate Problem Report within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:<br>• The nature of the alleged problem;<br>• The number of Certificate Problem Reports received about a particular Certificate or Subscriber;<br>• The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and<br>• Relevant legislation.<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.1.3) |
| 36 | The CA maintains controls to provide reasonable assurance that the CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.1.4) |
| 37 | The CA maintains controls to provide reasonable assurance that EV SSL Certificates are revoked within 24 hours if one or more of the following occurs:<br>• the Subscriber requests in writing that the CA revoke the Certificate;<br>• the Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;<br>• the CA obtains evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has suffered a Key Compromise, or that the Certificate has otherwise been misused (also see Baseline Requirements Section 10.2.4) or no longer complies with the requirements of Baseline Requirements Appendix A;<br>• the CA obtains evidence that the Certificate was misused;<br>• the CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement;<br>• the CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);<br>• the CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;<br>• the CA is made aware of a material change in the information contained in the Certificate;<br>• 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;<br>• the CA determines that any of the information appearing in the Certificate is inaccurate or misleading;<br>• the CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; |

| | |
|---|---|
| | • 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;<br>• the CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;<br>• revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or<br>• 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).<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.1.5 and Appendix A) |
| 38 | The CA maintains controls to provide reasonable assurance that it:<br>• has the capability to accept and acknowledge Certificate Problem Reports on a 24x7 basis;<br>• identifies high priority Certificate Problem Reports;<br>• begin investigation of Certificate Problem Reports within 24 hours:<br>• decides whether revocation or other appropriate action is warranted; and<br>• where appropriate, forwards such complaints to law enforcement.<br>(See EV SSL Guidelines Section 13 that refers to Baseline Requirements Section 13.1.1, 13.1.2, 13.1.3, and 13.1.4) |
| 39 | The CA maintains controls to provide reasonable assurance that ensure the system used to process and approve EV SSL Certificate Requests requires actions by at least two trusted persons before the EV SSL Certificate is created.<br>(See EV SSL Guidelines Section 16) |
| 40 | The CA maintains controls to provide reasonable assurance that:<br>• it performs ongoing self-audits against a randomly selected sample of at least three percent (3%) of the EV SSL Certificates issued. For all EV SSL Certificates where the final cross correlation and due diligence requirements of Section 24 of the EV SSL Guidelines are performed by an RA, this sample size is increased to six percent (6%).<br>• for new root keys generated after November 11, 2006 for the purpose of issuing EV SSL Certificates, the CA obtained an unqualified report from the CA's qualified auditor opining on the CA's root key and certificate generation process.<br>(See EV SSL Guidelines Section 17.5 and 17.7) |
| 41 | The CA maintains controls and procedures to provide reasonable assurance that:<br>• applicable requirements of the CA/Browser Forum Guidelines for Extended Validation Certificates are included (directly or by reference) in contracts with subordinate CAs, RAs, Enterprise RAs, and subcontractors that involve or relate to the issuance or maintenance of EV SSL Certificates, and<br>• the CA monitors and enforces compliance with the terms of the contracts.<br>(See EV SSL Guidelines Section 8.3) |

| | |
|---|---|
| 42 | The CA maintains controls to provide reasonable assurance that it complies with:<br>• laws applicable to its business and the certificates it issues in each jurisdiction where it operates, and<br>• licensing requirements in each jurisdiction where it issues EV SSL certificates.<br>(See EV SSL Guidelines Section 8.1) |
| 43 | The CA maintains controls and procedures to provide reasonable assurance that:<br>• the CA and Root CA maintain the minimum levels of Commercial General Liability Insurance (occurrence form) and Professional Liability/Errors & Omissions insurance as established by the EV SSL Guidelines, and<br>• the providers of the Insurance coverage meet the ratings qualifications established under the EV SSL Guidelines, or<br>• If the CA and/or its root CA self-insures for liabilities, the CA and/or its root CA maintains the minimum liquid asset size requirement established in the EV SSL Guidelines.<br>(See EV SSL Guidelines Section 8.4) |
| | **EMPLOYEE AND THIRD PARTY ISSUES** |
| 44 | With respect to employees, agents, or independent contractors engaged in the EV process, the CA maintains controls to:<br>• verify the identity of each person,<br>• perform background checks of such person to confirm employment, check personal references, confirm the highest or most relevant educational degree obtained and search criminal records where allowed in the jurisdiction where the person will be employed, and<br>• for employees at the time of the adoption of the EV SSL Guidelines by the CA verify the identity and perform background checks within three months of the date of the adoption of the EV SSL Guidelines.<br>(See EV SSL Guidelines Section 14.1.1) |
| 45 | The CA maintains controls to provide reasonable assurance that:<br>• The CA provides all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.<br>• The CA maintains records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.<br>• Validation Specialists engaged in Certificate issuance maintains skill levels consistent with the CA's training and performance programs.<br>• The CA documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.<br>The CA requires all Validation Specialists to pass an examination provided by the CA on the information |

| | |
|---|---|
| | verification requirements outlined in these Requirements<br><br>If a Delegated Third Party fulfils any of the CA's obligations under High Risk Requests, The CA maintains controls to provide reasonable assurance that verifies 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.)<br><br>(See EV SSL Guidelines Section 14.1.2 that refers to Baseline Requirements Section 14.1.2) |
| 46 | The CA maintains controls to provide reasonable assurance that there is a separation of duties such that no one person can both validate and authorize the issuance of an EV SSL Certificate.<br><br>(See EV SSL Guidelines Section 14.1.3) |
| 47 | The CA maintains controls to provide reasonable assurance that Certificate issuance by the Root CA requires that an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) deliberately issue a direct command in order for the Root CA to perform a certificate signing operation and that Root CA Private Keys are not used to sign EV SSL Certificates.<br><br>(See EV SSL Guidelines Section 12) |
| | **Data and Record Issues** |
| 48 | The CA maintains controls to provide reasonable assurance that the following EV key and certificate management events are recorded and maintained and the records maintained:<br><br>• CA key lifecycle management events, including:<br>  o key generation, backup, storage, recovery, archival, and destruction<br>  o cryptographic device lifecycle management events.<br>• CA and Subscriber EV SSL Certificate lifecycle management events, including:<br>  o EV SSL Certificate Requests, renewal and re-key requests, and revocation<br>  o all verification activities required by these Guidelines<br>  o date, time, phone number used, persons spoken to, and end results of verification telephone calls<br>  o acceptance and rejection of EV SSL Certificate Requests<br>  o issuance of EV SSL Certificates<br>  o generation of EV SSL Certificate revocation lists (CRLs) and OCSP entries.<br>• the CA maintains controls to provide reasonable assurance that following security events are recorded:<br>  o successful and unsuccessful PKI system access attempts<br>  o PKI and security system actions performed<br>  o security profile changes<br>  o system crashes, hardware failures, and other anomalies<br>  o firewall and router activities<br>  o entries to and exits from CA facility.<br>• Log entries includes the following elements:<br>  o Date and time of entry<br>  o Identity of the person making the journal entry<br>  o Description of entry |

| | |
|---|---|
| | (See EV SSL Guidelines Section 15 that refers to Baseline Requirements Section 15.2) |
| 49 | The CA and RA maintain controls to provide reasonable assurance that event logs at the CA and RA site are retained for at least seven years.<br>(See EV SSL Guidelines Section 15 that refers to Baseline Requirements Section 15.3.1) |
| 50 | The CA maintains controls to provide reasonable assurance that all previously revoked certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns are recorded in an internally managed database and used to flag suspicious EV SSL Certificate Requests.<br>(See EV SSL Guidelines Section 15 that refers to Baseline Requirements Section 15.3.2) |
| 51 | The CA has a policy to retain all documentation relating to all EV SSL Certificate Requests and verification thereof, and all EV SSL Certificates and revocation thereof, for at least seven years after any EV SSL Certificate based on that documentation ceases to be valid.<br>(See EV SSL Guidelines Section 15 that refers to Baseline Requirements Section 15.3.2) |
| 52 | The CA maintains controls to provide reasonable assurance that risks impacting its CA operations over EV certifications are assessed regularly and address the following:<br>• identify reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any EV Data or EV Processes;<br>• assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the EV Data and EV Processes; and<br>• assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to control such risks.<br>(See EV SSL Guidelines Section 16 that refers to Baseline Requirements Section 16.2) |
| 53 | The CA develops, implement, and maintain a Security Plan consisting of security, policies, procedures, measures, and products designed to reasonably manage and control the risks identified during the Risk Assessment.<br>(See EV SSL Guidelines Section 16 that refers to Baseline Requirements Section 16.3) |

**Appendix A**

# CA/Browser Forum

# Guidelines for the Issuance and Management of Extended Validation SSL Certificates

# Baseline Requirements

To download a copy of the current CA/Browser Forum EV SSL Certificate Guidelines Version 1.4.5 and the Baseline Requirements Version 1.1.6 go to:

**http://www.cabforum.org/documents**