WEBTRUST® FOR CERTIFICATION AUTHORITIES

WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES – EXTENDED VALIDATION SSL

Version 1.6.2

Release Date 1 October 2017

Effective Date For audit periods commencing on or after 1 November 2017

Based on the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation SSL Certificates – Version 1.6.2

Document History

Version	Publication Date	Revision Summary
1.4.5	3 April 2014	Updated EV SSL Audit Criteria to conform to EV SSL Guidelines v1.4.5
1.6.0	31 January 2017	Updated EV SSL Audit Criteria to conform to EV SSL Guidelines v1.6.0, including remapping all Baseline criteria reference numbers as the SSL Baseline Requirements were updated to conform to RFC 3647. The numbering scheme of the criteria in Principle 2 was updated in order to better relate similar criterion to each other. Additionally, the following changes were made: • Principle 2, Criteria Section 1.x – Moved criteria relating to key generation ceremonies here • Principle 2, Criterion 2.1.1 – Spilt to 4 criterion (2.1.1 to 2.1.4) • Principle 2, Criterion 4.3 – Change verification of phone number to Verified Method of Communication • Principle 2, Criterion 4.4 – Changes to the definition of 'Operational Existence' and acceptable methods of verification • Principle 2, Criterion 4.5 – Expanded the definition of 'Applicant' to include Parent Company, Subsidiaries, and Affiliates, referenced out to SSL Baseline Section 3.2.2.4. • Principle 2, Criterion 4.6 – Added verification requirements for .onion domains • Principle 2, Criterion 4.14 – Clarified criteria • Principle 2, Criterion 4.19 – Clarified criteria and updated references • Principle 2, Criteria Section 5.x – Aligned wording to the SSL Baseline Audit Criteria v2.1. • Principle 2, Criteria Section 5, 6, and 7 – Moved some criteria to Section 4 to better group similar criteria • Principle 2, Criteria Section 8.x – Relocated all audit and legal related criteria to this section
1.6.2	1 October 2017	Updated EV SSL Audit Criteria to conform to EV SSL Guidelines v1.6.2 and other clarifications, including the following • Principle 2, Criterion 2.2.3 – Updated maximum EV certificate lifetime to 825 days • Principle 2, Criterion 4.13 – Codified the requirements regarding the CA's responsibility for verifying the accuracy of QIISs used for verification

Acknowledgements

This document has been prepared by the WebTrust/PKI Assurance Task Force (the "Task Force") for use by those auditors licensed to perform WebTrust for Certification Authorities audits by CPA Canada.

Members of the Task Force are:

- Jeffrey Ward, *BDO USA, LLP* (Chair)
- Donald E. Sheehy (Vice-Chair)
- Chris Czajczyc, *Deloitte LLP*
- Reema Anand, *KPMG LLP*
- David Roque, *Ernst & Young LLP*

Significant support has been provided by:

- Daniel J. Adam, *Deloitte & Touche LLP*
- Donoghue Clarke, *Ernst & Young LLP*
- Timothy Crawford, *BDO USA, LLP*
- Zain Shabbir, *KPMG LLP*

CPA Canada Support

- Kaylynn Pippo, (Staff Contact)
- Bryan Walker, Consultant
- Janet Treasure, Vice President, Member Development and Support
- Gord Beal, Vice President, Research, Guidance and Support

Table of Contents

Introduction

The primary goal of the CA/Browser Forum's ("Forum") Guidelines for the Issuance and Management of Extended Validation (EV) SSL Certificates ("EV SSL Guidelines") is to enable efficient and secure electronic communication, whilst addressing user concerns about the trustworthiness of Certificates. The Guidelines also serve to inform users and help them to make informed decisions when relying on Certificates.

The CA/Browser Forum, that consists of many of the issuers of digital certificates and browser and other application developers, has developed guidelines that set out the expected requirements for issuing and managing EV SSL[1] Certificates (the "EV SSL Guidelines").

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

Extended Validation overview

The growth of internet transactions has emphasised the importance of strong authentication of the identity of websites, domain owners, online servers, and software code. 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.

Browsers and software developers often provide EV Certificates with elevated status within their applications, for example, through the use of favourable user interface elements, or in some cases prohibiting the use of non-EV Certificates.

Adoption and effective dates

These Audit Criteria incorporate and make reference to relevant CA/Browser Forum Guidelines and Requirements as listed in Appendix A, and are effective for audit periods commencing on or after 1 Novemb 2017.

The Forum may periodically publish updated Guidelines and Requirements. The auditor is not required to consider these updated versions until reflected in the subsequently updated Audit Criteria.

In certain instances, the Forum updates its Guidelines and Requirements with certain criteria only effective at a date later than the publication date. The auditor is directed to review the document

[1] The term SSL is used to refer to certificates intended to authenticate servers, based on the original SSL protocol which was used. Modern browser and application deployments make use of newer technologies such as TLS, and are equally in scope for these requirements.

history, revisions, and relevant dates in the Forum documents to understand the applicability of certain Guidelines and Requirements.

For a list of Forum Guidelines and Requirements that have effective dates later than the effective date of these Audit Criteria, refer to Appendix D.

References to SSL Baseline Requirements

In 2011, the CA/Browser Forum introduced its Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements", "SSL Baseline Requirements" or "BRs"). Since that time, the Forum has worked to harmonise its EV SSL Guidelines with the SSL Baseline Requirements by aligning criteria and in many instances referencing the EV SSL Guidelines directly to applicable sections in the SSL Baseline Requirements.

These Audit Criteria include references to both the relevant sections of the EV SSL Guidelines and the SSL Baseline Requirements for each criterion as applicable, and the auditor is directed to consider both of these in performing its audit.

For the SSL Baseline Requirements, the auditor is directed to consider the version as outlined in Appendix A.

Connection with WebTrust for CA

These Audit Criteria are designed to be used in conjunction with an audit of a CA as required by the CA/Browser Forum. Due to significant overlap between these Audit Criteria and the WebTrust Principles and Criteria for Certification Authorities Version 2.x or later ("WebTrust for CA" or "WTCA"), this audit should be conducted simultaneously with the WebTrust for CA audit.

Requirements not subject to audit

In preparing these Audit Criteria, the Task Force reviewed the relevant CA/Browser Forum documents as outlined in Appendix A, with the intent of identifying items that would not be subject to audit. The results of this review are set out in Appendix B.

Principle 1: 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.

#	Criterion	Ref[2]	SSL BR Ref[3]
1	The CA and its Root CA discloses[4] on its website: • EV SSL Certificate practices, policies and procedures; • CAs in the hierarchy whose subject name is the same as the EV SSL issuing CA; and • its commitment to conform to the latest version of the Guidelines for Issuance and Management of Extended Validation Certificates issued by the CA/Browser Forum.	8.2.2, 8.3	N/A
2	The Certificate Authority has published guidelines for revoking EV SSL Certificates	13	4.9
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.	13	4.9
4	The CA and its Root has controls to provide reasonable assurance that there is public access to the CP and/or CPS on a 24x7 basis, and the content and structure of the CP and/or CPS are in accordance with either RFC 2527 or RFC 3647.	8.2.2	N/A

[2] Reference to the applicable section(s) of the Extended Validation SSL Guidelines for this criterion. The auditor is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion.
[3] Reference to the applicable section(s) of the SSL Baseline Requirements for this criterion. The auditor is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion.
[4] The criteria are those that are to be tested for the purpose of expressing an opinion on these WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL. 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: Extended Validation SSL Service Integrity

The Certification Authority (CA) maintains effective controls to provide reasonable assurance that:

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

#	Criterion	Ref[5]	SSL BR Ref[6]
	KEY GENERATION CEREMONIES		
1.1	The CA maintains controls to provide reasonable assurance that Root CA and Subordinate CA Key Pairs used for EV SSL Certificates are created in accordance with SSL Baseline Requirements Section 6.1.1.1.	17.7	6.1.1.1
1.2	The CA maintains controls to provide reasonable assurance that Root CA Key Pairs used for EV SSL certificates created on or after 11 November 2006 are: • Witnessed by the CA's Qualified Auditor; and • Receive a Unqualified Audit Opinion from the CA's Qualified Auditor opinion on the CA's root key and certificate generation process.	17.7	N/A
	EV SSL SUBSCRIBER AND CERTIFICATE CONTENT PROFILES		
	Subscriber Profile		
2.1.1	The CA maintains controls to provide reasonable assurance that it issues EV SSL Certificates to Private Organizations as defined within the EV SSL Guidelines that meet the following requirements: • 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); • the entity designated with the Incorporating or Registration	8.5.2	N/A

[5] Reference to the applicable section(s) of the Extended Validation SSL Guidelines for this criterion. The auditor is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion.
[6] Reference to the applicable section(s) of the SSL Baseline Requirements for this criterion. The auditor is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion.

	Agency a Registered Agent, or a Registered Office (as required under the laws of the jurisdiction of Incorporation or Registration), or an equivalent facility; • the entity is not designated as inactive, invalid, non-current or equivalent in records of the Incorporating Agency or Registration Agency; • the entity has a verifiable physical existence and business presence; • 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 • 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.		
2.1.2	The CA maintains controls to provide reasonable assurance that it issues EV SSL Certificates to Government Entities as defined within the EV SSL Guidelines that meet the following requirements: • the entity's legal existence was established by the political subdivision in which the entity operates; • 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 • 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.	8.5.3	N/A
2.1.3	The CA maintains controls to provide reasonable assurance that it issues EV SSL Certificates to Business Entities as defined within the EV SSL Guidelines that meet the following requirements: • 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; • the entity has a verifiable physical existence and business presence; • at least one Principal Individual associated with the entity(owners, partners, managing members, directors or officers) is identified and validated by the CA; • the identified Principal Individual (owners, partners, managing members, directors or officers) attests to the representations made in the Subscriber agreement; • the CA verifies the entity's use of any assumed name, used to represent the entity pursuant to the requirements of Section 11.3; • 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	8.5.4	N/A

	• 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.		
2.1.4	The CA maintains controls to provide reasonable assurance that it issues EV SSL Certificates to Non-Commercial Entities as defined within the EV SSL Guidelines that meet the following requirements: • 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; • 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 • 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.	8.5.5	N/A
	Certificate Content and Profile		
2.2.1	The CA maintains controls to provide reasonable assurance that 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: • Issuer Common Name Field • Issuer Domain Component Field • Issuer Organization Name Field • Issuer Country Name Field • Full legal organization name and if space is available the d/b/a name may also be disclosed • Subject Alternative Name Extension • Subject Common Name Field • Subject Business Category Field • Subject Jurisdiction of Incorporation or Registration Field • Subject Registration Number Field • Subject Physical Address of Place of Business Field • Other Subject Attributes	9, 9.1	7.1.4.1
2.2.2	The CA maintains controls to provide reasonable assurance that EV SSL Certificates issued include the minimum requirements for the content of EV SSL Certificates, including: • Certificate Policy Identification requirements • Subscriber Public Key • Certificate Serial Number • Additional Technical Requirements for EV Certificates	9.3.2, 9.3.4, 9.3.5, 9.5, 9.6, 9.7	6.1.1.3, 6.1.5, 7.1

	as established in the EV SSL Guidelines relating to: • EV SSL Subscriber Certificates • EV Subordinate CA Certificates		
2.2.3	The CA maintains controls to provide reasonable assurance that EV SSL Subscriber Certificates are valid for a period not exceeding 825 days.	9.4	N/A
2.2.4	The CA maintains controls to provide reasonable assurance that the data that supports the EV SSL Certificates is revalidated within the timeframes established in the EV SSL Guidelines.	11.14	N/A
	EV SSL CERTIFICATE REQUEST REQUIREMENTS		
3.1	The CA maintains controls to provide reasonable assurance that the EV SSL Certificate Request is: • obtained and complete prior to the issuance of EV SSL Certificates; • signed by an authorized individual (Certificate Requester); • approved by an authorized individual (Certificate Approver) • properly certified as to being correct by the applicant; and • contains the information specified in Section 10 of the EV SSL Guidelines	10, 10.2	4.1.2
	Subscriber Agreements and Terms of Use		
3.2	The CA maintains controls to provide reasonable assurance that the CA, prior to the issuance of a EV SSL Certificate, obtains a Subscriber and/or Terms of Use agreement in accordance with the EV SSL Guidelines. That agreement is: • signed by an authorized contract signer; • names the applicant and individual contract signer; and • contains provisions imposing obligations and warranties on the Application relating to: o the accuracy of information o protection of Private Key o acceptance of the EV SSL certificate o use of the EV SSL certificate o reporting and revocation upon compromise o termination of use of the EV SSL certificate o responsiveness o acknowledgement and acceptance.	10.3	9.6.3
	INFORMATION VERIFICATION REQUIREMENTS		
	Verification of Applicant's Legal Existence and Identity		
4.1	The CA maintains controls 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:	11.1, 11.2, 11.3,	N/A

	For Private Organization Subjects:
	
	• legal existence and identity
	• legal existence and identity – assumed name
	• organization name
	• registration number
	• registered agent
	• relationship to the parent, subsidiary, or affiliate (if applicable)
	
	For Government Entities:
	
	• legal existence
	• entity name
	• registration number
	
	For Business Entities:
	
	• legal existence
	• organization name
	• registration number
	• principal individual
	• relationship to the parent, subsidiary, or affiliate (if applicable)
	
	For Non-Commercial Entities:
	
	• International Organization Entities
	  o legal entities
	  o entity name
	  o registration number
		11.12.3	

	Verification of Applicant		
4.2	The CA maintains controls 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.	11.4.1	N/A
4.3	The CA maintains controls to provide reasonable assurance that it verifies a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant by performing the steps set out in the EV SSL Guidelines.	11.5.1	N/A
4.4	The CA maintains controls to provide reasonable assurance that it verifies the Applicant has the ability to engage in business by verifying the Applicant's, or Affiliate/Parent/Subsidiary Company's, operational existence by: • verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years,	11.6	N/A

	as indicated by the records of an Incorporating Agency or Registration Agency; • verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current QIIS or QTIS; • verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution; or • relying 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.		
4.5	The CA maintains controls to provide reasonable assurance that for each Fully-Qualified Domain Name listed in a Certificate, other than a Domain Name with .onion in the rightmost label of the Domain Name, 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") either is the Domain Name Registrant or has control over the FQDN by using a procedure specified in Section 3.2.2.4 of the SSL Baseline Requirements.	11.7.1	3.2.2.4
4.6	The CA maintains controls to provide reasonable assurance that for a Certificate issued to a Domain Name with .onion in the right-most label of the Domain Name, the CA confirms that, as of the date the Certificate was issued, the Applicant's control over the .onion Domain Name in accordance with Appendix F of the EV SSL Guidelines.	App. F	N/A
	Verification of Other		
4.7	The CA maintains controls to provide reasonable assurance that the CA uses an internal database of all previously revoked Certificates and previously rejected certificate requests to identify subsequent suspicious certificate requests.	11.12.1	4.1.1
4.8	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: • 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; and • the CA shall use information identified by the CA's high-risk criteria to flag suspicious certificate requests. The CA shall follow a documented procedure for performing additional verification of any certificate request flagged as suspicious or high risk.	11.12.1	4.2.1

4.9	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: • 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 • 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.	11.12.2	N/A
	Verification of Contract Signer and Approver		
4.10	The CA maintains controls to provide reasonable assurance that it verifies, using a method of verification established by the EV SSL Guidelines: • 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; • 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"); • 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: o submit, and if applicable authorize a Certificate Requester to submit, the EV SSL Certificate Request on behalf of the Applicant; o 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 o approve EV SSL Certificate Requests submitted by a Certificate Requester.	11.8	N/A
	Verification of EV SSL Certificate Requests		
4.11	The CA maintains controls to provide reasonable assurance, using a method of verification established in the EV SSL Guidelines that: • subscriber Agreements are signed by an authorized Contract signer; • the EV SSL Certificate Request is signed by the Certificate Requester submitting the document; • if the Certificate requester is not also an authorized Certificate Approver, an authorized Certificate Approver independently	11.9, 11.10	N/A

	approves the EV SSL Certificate Request unless pre-authorized; and • signatures have been properly authenticated.		
4.12	The CA maintains controls to provide reasonable assurance that in cases where an EV SSL Certificate Request is submitted by a Certificate Requester, before it issues the requested EV SSL Certificate, it verifies that an authorized Certificate Approver reviewed and approved the EV SSL Certificate Request.	11.10	N/A
4.13	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: • with respect to legal opinions; o the independent status of the author, o the basis of the opinion, and o authenticity. • with respect to accountants letters; o the status of the author, o the basis of the opinion, and o authenticity. • with respect to face-to-face vetting documents; o qualification of third-party validator, o document chain of custody, and o verification of attestation. • with respect to independent confirmation from applicant; o the request is initiated by the CA requesting verification of particular facts, o 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. o the Confirming Person confirms the fact or issue. • with respect to Qualified Independent Information Sources (QIIS) o the database used is a QIIS as defined by the EV SSL Guidelines 11.11.5. o the CA follows a documented process to check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider's terms of use o the CA does not use any data in a QIIS that the CA knows is (i) self-reported and (ii) not verified by the QIIS as accurate • with respect to Qualified Government Information Sources (QGIS) o the database used is a QGIS as defined by the EV SSL Guidelines 11.11.6. • with respect to Qualified Government Tax Information Source (QGTIS) o a Qualified Governmental information source is used that specifically contains tax information relating to Private	11.11, 11.11.5, 11.11.6, 11.11.7, 11.14	N/A

	Organizations, Business Entities or Individuals as defined by the EV SSL Guidelines 11.11.7.		
	Validation for Existing Subscribers		
4.14	The CA maintains controls to provide reasonable assurance that 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, subject to any exceptions as outlined in Section 11.14.1 and re-issuance requests in Section 11.14.2.	11.14, 11.14.1, 11.14.2	N/A
	Segregation of Duties		
4.15	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.	16	N/A
4.16	The CA maintains controls to provide reasonable assurance that there is a separation of duties such that no one person can both validate and authorise the issuance of an EV SSL Certificate.	14.1.3	N/A
	Certificate Issuance by a Root CA		
4.17	The CA maintains controls to provide reasonable assurance that 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.	12	4.3.1
4.18	The CA maintains controls to provide reasonable assurance that Root CA Private Keys are not used to sign EV SSL certificates.	12	N/A
	Other Matters		
4.19	The CA maintains controls to provide reasonable assurance that except for certificate requests approved by an Enterprise Registration Authority ("RA"): • 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; • any identified discrepancies are documented and resolved before certificate issuance; and • 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	11.13, 14.1.2, 14.1.3, 17.5, 17.6	N/A

	identification and authorization and fulfilling all qualification requirements contained in Section 14.1. When employees do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA may: o rely on the translations by a Translator or, if an RA is used, the CA must review the work completed by the RA and determine that all requirements have been met; and o The CA may rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with its requirements and is subjected to the Audit Requirements of Sections 17.5 and 17.6 as specified in the EV SSL Guidelines.		
CERTIFICATE REVOCATION AND STATUS CHECKING			
5.1	The CA maintains controls to provide reasonable assurance that a process is available 24x7 that the CA is able to accept and respond to revocation requests and related inquiries, and that the CA provides a process for Subscribers to request revocation of their own certificates.	13	4.9.3
5.2	The CA maintains controls to provide reasonable assurance that it: • has the capability to accept and acknowledge Certificate Problem Reports on a 24x7 basis; • identifies high priority Certificate Problem Reports; • begin investigation of Certificate Problem Reports within 24 hours; • decides whether revocation or other appropriate action is warranted; and • where appropriate, forwards such complaints to law enforcement.	13	4.9.3, 4.9.5, 4.10.2
5.3	The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6; 4. The CA obtains evidence that the Certificate was misused; 5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use Agreement; 6. 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	13	4.9.1.2, 6.1.5, 6.1.6

	Name Registrant has failed to renew the Domain Name); 7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; 8. The CA is made aware of a material change in the information contained in the Certificate; 9. 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; 10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; 12. 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; 13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate; 14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or 15. 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).		
5.4	The CA maintains controls to provide reasonable assurance that Subordinate CA Certificates are revoked within 7 days if any of the following events occurs: 1. The Subordinate CA requests revocation in writing; 2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6; 4. The Issuing CA obtains evidence that the Certificate was misused; 5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with these Baseline Requirements or the applicable Certificate Policy or Certification Practice Statement; 6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; 8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated,	13	4.9.1.2, 6.1.5, 6.1.6

	unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; 9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or 10. 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.		
5.5	The CA maintains controls to provide reasonable assurance that the CA: • makes revocation information available via the cRLDistributionPoints and/or authorityInformationAccess certificate extensions for Subordinate CA and Subscriber Certificates in accordance with the SSL Baseline Requirements Section 7.1.2; and • for high-traffic FQDNs, distributes its OCSP responses in accordance with SSL Baseline Requirements.	13	7.1.2, 4.9.11
5.6	The CA maintains controls to provide reasonable assurance that an online 24x7 Repository is provided that application software can use to automatically check the current status of all unexpired Certificates issued by the CA, and: • for the status of Subscriber Certificates: o If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven (7) days, and the value of the nextUpdate field must not be more than ten (10) days beyond the value of the thisUpdate field; and o The CA shall update information provided via an Online Certificate Status Protocol (OCSP) at least every four (4) days and OCSP responses must have a maximum expiration time of ten (10) days. • for the status of subordinate CA Certificates o The CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field; and o The CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate. • The CA makes revocation information available through an OCSP capability using the GET method for Certificates issued in accordance with the SSL Baseline Requirements.	13	4.10.2, 4.9.7, 4.9.10

5.7	The CA maintains controls to provide reasonable assurance that the CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.	13	4.10.2
5.8	The CA maintains controls to provide reasonable assurance that the CA does not remove revocation entries on a CRL or OCSP Response until after the Expiry Date of the revoked Certificate.	13	4.10.1
5.9	The CA maintains controls to provide reasonable assurance that OCSP responses conform to RFC6960 and/or RFC5019, and are signed either: • by the CA that issued the Certificates whose revocation status is being checked, or • by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked (the OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960).	13	4.9.9
5.10	The CA maintains controls to provide reasonable assurance that OCSP responses by CA's which have not been technically constrained in accordance with SSL Baseline Requirements Section 7.1.5 do not respond with a "good" status for Certificates that have not been issued.	13	4.9.10
5.11	The CA maintains controls to provide reasonable assurance that CRLs for an EV SSL Certificate chain can be downloaded in no more than three (3) seconds over an analogue telephone line under normal network conditions.	13	N/A
	EMPLOYEES AND THIRD PARTIES		
6.1	The CA maintains controls to provide reasonable assurance that with respect to employees, agents, or independent contractors engaged in the EV process, the CA: • verifies the identity of each person; • performs background checks of such person to confirm employment, checks personal references, confirms the highest or most relevant educational degree obtained and searches criminal records where allowed in the jurisdiction where the person will be employed; and • for employees at the time of the adoption of the EV SSL Guidelines by the CA, verifies the identity and perform background checks within three months of the date of the adoption of the EV SSL Guidelines.	14.1.1	N/A
6.2	The CA maintains controls to provide reasonable assurance that: • the CA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic	14.1.2	5.3.3, 5.3.4

	Public Key Infrastructure (PKI) 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; • the CA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily; • the CA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task; • the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements; and • all personnel in Trusted Roles maintain skill levels consistent with the CA's training and performance programs.		
6.3	The CA maintains controls to provide reasonable assurance that Delegated Third Parties meet the qualification requirements of Section 14.1 of the EV SSL Guidelines.	14.2.1, 14.1	N/A
6.4	The CA maintains controls to provide reasonable assurance that the CA verifies that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 (SSL Baseline 5.3.3) and the document retention and event logging requirements of Section 15 (SSL Baseline 5.4.1).	14.2.1	5.3.7, 5.3.3, 5.4.1
6.5	For High Risk Certificate Requests, the CA maintains controls to provide reasonable assurance that the CA verifies that the Delegated Third Party's processes to identify and further verify High Risk Certificate Requests meets the requirements of the CA's own processes for High Risk Certificate Requests.	14.1.2	4.2.1
	DATA RECORDS		
7.1	The CA maintains controls to provide reasonable assurance that the CA records details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved.	15	5.4.1
7.2	The CA maintains controls to provide reasonable assurance that the following events are recorded: • CA key lifecycle management events, including: o key generation, backup, storage, recovery, archival, and destruction o cryptographic device lifecycle management events. • CA and Subscriber Certificate lifecycle management events, including: o Certificate Requests, renewal and re-key requests, and revocation	15	5.4.1

	○ all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement ○ date, time, phone number used, persons spoken to, and end results of verification telephone calls ○ acceptance and rejection of certificate requests ○ issuance of Certificates ○ generation of Certificate Revocation Lists (CRLs) and OCSP entries. • security events, including: ○ successful and unsuccessful PKI system access attempts ○ PKI and security system actions performed ○ security profile changes ○ system crashes, hardware failures, and other anomalies ○ firewall and router activities ○ entries to and exits from CA facility. • Log entries must include the following elements: ○ Date and time of entry ○ Identity of the person making the journal entry ○ Description of entry		
7.3	The CA maintains controls to provide reasonable assurance that audit logs are retained for at least seven years.	15	5.4.3
7.4	The CA maintains controls to provide reasonable assurance that all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, is retained for at least seven years after any Certificate based on that documentation ceases to be valid.	15	5.5.2
	AUDIT AND LEGAL		
8.1	The CA maintains controls to provide reasonable assurance that: • it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the EV SSL Certificates issued during the period commencing immediately after the previous self-assessment samples were taken. For all EV SSL certificates where the final cross-correlation and due diligence requirements of Section 11.13 are performed by a Delegated Third Party, the sample size is increased to at least six percent (6%); and • The CA reviews each Delegated Third Party's practices and procedures to assess that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.	17.5	N/A
8.2	The CA maintains controls to provide reasonable assurance that: • 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,	8.3, 14.2, 14.2.3	N/A

	and subcontractors that involve or relate to the issuance or maintenance of EV SSL Certificates, and that they are contractually obligated to comply with the applicable requirements in the EV SSL Guidelines and to perform them as required of the CA itself; • the CA monitors and enforces compliance with the terms of the contracts; and • the CA annually internally audits compliance with the EV SSL Guidelines.		
8.3	The CA maintains controls to provide reasonable assurance that it complies with: • laws applicable to its business and the certificates it issues in each jurisdiction where it operates, and • licensing requirements in each jurisdiction where it issues EV SSL certificates.	8.1	8.0
8.4	The CA maintains controls and procedures to provide reasonable assurance that: • 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 • the providers of the Insurance coverage meet the ratings qualifications established under the EV SSL Guidelines, or • 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.	8.4	N/A

Appendix A: CA/Browser Forum Documents

These Audit Criteria are based on the following CA/Browser Forum Documents:

Document Name	Version	Effective Date
Guidelines for the Issuance and Management of Extended Validation SSL Certificates	1.6.2	17 March 2017
Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	1.4.9	11 July 2017

Copies of these documents are available on the CA/Browser Forum's website at:
https://cabforum.org/documents

Appendix B: Sections of the EV SSL Guidelines not subject to audit

Sections of the EV SSL Guidelines which contain no content or the phrase 'No Stipulation' were not considered for audit. Additionally, the following items are not subject to audit:

Ref	Topic	Reasons for exclusion
1	Scope	Information only, no auditable items
2	Purpose	Information only, no auditable items
3	References	Information only, no auditable items
4	Definitions	No auditable items, however the auditor is directed to consider these definitions when interpreting the EV SSL Guidelines and these audit criteria.
5	Abbreviations and Acronyms	Information only, no auditable items
6	Conventions	Information only, no auditable items
7	Certificate Warranties and Representations	Legal item
16	Data Security	References to SSL Baseline Section 5 are addressed in *WebTrust Principles and Criteria – SSL Baseline with Network Security,* Principles 3 and 4, and are not subject to audit in these audit criteria.
17 (except 17.5, 17.7)	Audit	Information only, no auditable items
18	Liability and Indemnification	Legal item
App. B	Sample Attorney Opinions Confirming Specified Information	Information only, no auditable items
App. C	Sample Accountant Letters Confirming Specified Information	Information only, no auditable items
App. D	Country-Specific Interpretative Guidelines	No auditable items, however the auditor is directed to consider details surrounding non-Latin organisation names, Romanised names, translated names, and country-specific requirements as applicable.
App. E	Sample Contract Signer's	Information only, no auditable items

	Representation/Warranty	

Appendix C: Unused

This section is currently unused.

Appendix D: CA/Browser Forum effective date differences

SSL Baseline Requirements

The following Baseline Requirements have effective dates later than the effective date of these Audit Criteria. Refer to details and instructions below for guidance on how to address these as part of an audit:

Ref	Effective Date	Guidance
1.5.2	3 December 2016	The requirements specified in this section need only be considered as of 3 December 2016 onwards.
2.3	3 December 2016	The requirements specified in this section need only be considered as of 3 December 2016 onwards.
2.4	3 December 2016	The requirements specified in this section need only be considered as of 3 December 2016 onwards.
3.2.2.4	1 March 2017	Baseline Requirements v1.3.8 replaced the entirety of the domain validation requirements in this section with new requirements. For certificates issued on or before 28 February 2017, the auditor is directed to consider the domain validation requirements in Section 3.2.2.4 of Baseline Requirements v1.3.7. For certificates issued on or after 1 March 2017, the auditor is directed to consider the domain validation requirements in Section 3.2.2.4 of Baseline Requirements v1.4.1.

EV SSL Guidelines

No differences.