# WebTrust[SM/TM] for Certification Authorities

# WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0

**Based on:**

## *CA/Browser Forum*

## *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates – Version 1.1.6*

***AND***

## *Network and Certificate Systems Security Requirements – Version 1.0*

## RELEASE DATE

April 3, 2014

## EFFECTIVE DATE

Audit periods starting on or after July 1, 2014

# TABLE OF CONTENTS

This document has been prepared for the use by those auditors licensed to perform SSL Baseline Requirements audits by the CPA Canada.

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

| | |
|---|---|
| **Chair**<br>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* | **Staff Contact:**<br><br>Bryan Walker<br>*CPA Canada* |

The Task Force would like to thank Robert Ikeoka, KPMG LLP, Donoghue Clarke, Ernst & Young LLP, and Daniel J. Adam, Deloitte LLP for their contributions in the preparation of this guide. The Task Force would also like to express its appreciation to the contribution 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.

# INTRODUCTION

The primary goal of the CA/Browser Forum "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.6" and "Network and Certificate Systems Security Requirements, v.1.0" is to enable efficient and secure electronic communication, while addressing user concerns about the trustworthiness of SSL Certificates. The Requirements also serve to inform users and help them to make informed decisions when relying on SSL Certificates.

The CA/Browser Forum, that consists of many of the issuers of digital certificates and browser developers, has developed guidelines that set out the expected requirements for issuing SSL certificates. The guidelines entitled "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" were recently updated to version 1.1.6 ("SSL Baseline Requirements"). The Forum has also issued additional security guidelines "Network and Certificate Systems Security Requirements" published at version 1.0 can be found at http://www.cabforum.org/. These Network and Certificate System Security Requirements (NCSS Requirements) apply to all publicly trusted Certification Authorities (CAs).

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 SSL Baseline Guidelines and NCSS Requirements includes requirements for CAs that wish to issue SSL certificates.

The purpose of these WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security ("Baseline and Network Criteria") is to set out criteria that would be used as a basis for an auditor to conduct a SSL Baseline Requirements and Network and Certificate Systems Security Requirements audit.

### *Adoption*

Version 1.1.6 of the SSL Baseline Requirements was published effective 29 July 2013. Version 1.0 of the Network and Certificate System Security Requirements was published with an effective date of 1 January 2013. WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0 is effective for periods beginning on or after 1 July 2014, however earlier implementation to coincide with the effective date of the relevant version of the SSL Baseline Requirements and Network and Certificate System Security Requirements is encouraged.

The CA/Browser Forum may periodically publish updated versions of the SSL Baseline Requirements and Network and Certificate Systems Security Requirements. The auditor is not required to consider these updated versions until reflected in the subsequently updated audit criteria.

As mentioned, the Baseline and Network Criteria are to be used only in conjunction with an audit of the Certification Authority as required by the CA/Browser Forum Guidelines. Due to the significant overlaps between these Baseline and Network Criteria and WebTrust for Certification Authorities (based on the WebTrust Principles and Criteria for Certification Authorities Version 2.0), this audit should be conducted simultaneously with the WebTrust for CA audit.

[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.

If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 17.1 of the SSL Baseline Requirements, then before issuing Publicly-Trusted SSL Certificates, the CA shall successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 17.1 of the SSL Baseline Requirements. The point-in-time readiness assessment shall be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and shall be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate. (See SSL Baseline Requirements Section 17.4) To satisfy this requirement a point-in-time audit is performed.

If, in the auditor's opinion, one or more of the criteria is not met, a reservation (qualification) of opinion should be included in the audit report. If a qualified report is issued, the CA would not be issued or permitted to display a WebTrust Baseline seal.

In preparing the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0, the Task Force reviewed the CA/Browser Forum's SSL Baseline Requirements for the Issuance and Management for Publicly-Trusted Certificates, V1.1.6 and Network and Certificate System Security Requirements V1.0 with the intent of identifying those requirements that would not be included in an audit. The results of this review are set out in Appendices B and C.

### *References*

In this document, any references to WebTrust for Certification Authorities (WTCA) refer to audits conducted in accordance with the WebTrust Principles and Criteria for Certification Authorities Version 2.0.

# WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

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

| | |
|---|---|
| 1 | The CA discloses[2] on its website its:<br>• Certificate practices, policies and procedures,<br>• all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue), and<br>• its commitment to conform to the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum.<br><br>(See SSL Baseline Requirements Section 8.3 and 8.4) |
| 2 | The Certificate Authority discloses in the Certificate Policy (CP) and/or Certification Practice Statement (CPS) that it includes its limitations on liability, if the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement.<br>(See SSL Baseline Requirements Section 18.1) |
| 3 | The issuing CA documents in its CP or CPS that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with the SSL Baseline Requirements.<br>(See SSL Baseline Requirements Section 9.3.4) |
| 4 | The Certificate Authority has controls to provide reasonable assurance that the CA CP and/or CPS that describes how the CA implements the latest version of the Baseline Requirements are updated annually.<br>(See SSL Baseline Requirements Section 8.2.1) |

[2] The criteria are those that are to be tested for the purpose of expressing an opinion on Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security. 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 SSL Baseline Requirements.

| | |
|---|---|
| 5 | 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. (See SSL Baseline Requirements 8.2.2) |

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

- Ï 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 certificates it manages is established and protected throughout their life cycles.

| | |
|---|---|
| | The following criteria apply to both new and renewed Certificates. |
| 1 | **Key Generation Ceremony** |
| 1.1 | The CA maintains controls to provide reasonable assurance that for Root CA Key Pairs created after the Effective Date of the Baseline Requirements that Baseline Requirements are followed.<br>(See SSL Baseline Requirements Section 17.7) |
| 2 | **CERTIFICATE CONTENT AND PROFILE** |
| 2.1 | The CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the Baseline Requirements including the following:<br>• Issuer Information (See SSL Baseline Requirements Section 9.1)<br>• Subject Information (See SSL Baseline Requirements Section 9.2)<br>• Certificate Policy Identification (See SSL Baseline Requirements Section 9.3)<br>• Validity Period (See SSL Baseline Requirements Section 9.4)<br>• Public Key (See SSL Baseline Requirements Section 9.5)<br>• Certificate Serial Number (See SSL Baseline Requirements Section 9.6)<br>• Additional Technical Requirements (See SSL Baseline Requirements Section 9.7)<br>o Appendix A - Cryptographic Algorithm and Key Requirements<br>o Appendix B - Certificate Extensions.<br>(See SSL Baseline Requirements Section 9) |
| 2.2 | The CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the SSL Baseline Requirements including the following:<br>• As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA shall notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. Also as of the Effective Date, the CA shall not issue a certificate with an Expiry Date later than 1 November 2015 with a |

| | |
|---|---|
| | subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, CAs shall revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name.<br><br>(See SSL Baseline Requirements Section 9.2.1) |
| 2.3 | The CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the SSL Baseline Requirements including the following:<br>• The CA shall implement a process that prevents an OU attribute from including a name, DBA, trade name, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with SSL Baseline Requirements Section 11.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with SSL Baseline Requirements Section 11.2.<br>• Appendix C - User Agent Verification.<br><br>(See SSL Baseline Requirements Section 9.2.6) |
| 2.4 | The CA maintains controls and procedures to provide reasonable assurance that Subscriber Certificates are valid for a period in accordance with SSL Baseline Requirements Section 9.4.<br><br>(See SSL Baseline Requirements Section 9.4) |
| 2.5 | The CA maintains controls and procedures to provide reasonable assurance that Certificates are not issued if the requested Public Key does not meet the requirements set forth in Appendix A or if it has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).<br><br>(See SSL Baseline Requirements Section 9.5) |
| 3 | **CERTIFICATE REQUEST REQUIREMENTS** |
| 3.1 | The CA maintains controls and procedures to provide reasonable assurance that the CA, prior to the issuance of a Certificate obtains the following documentation from the Applicant:<br>1. A certificate request, which may be electronic; and<br>2. An executed Subscriber or Terms of Use Agreement, which may be electronic.<br>3. Any additional documentation the CA determines necessary to meet the Baseline Requirements. |

| | |
|---|---|
| | (See SSL Baseline Requirements Section 10.1) |
| 3.2 | The CA maintains controls and procedures to provide reasonable assurance that the Certificate Request is:<br>• obtained and complete prior to the issuance of Certificates (See Baseline Requirements Section 10.2.1),<br>• signed by an authorized individual (Certificate Requester),<br>• properly certified as to being correct by the applicant (See SSL Baseline Requirements Section 10.2.2), and<br>• contains the information specified in Section 10.2.3 of the SSL Baseline Requirements. |
| | **Subscriber Private Keys** |
| 3.3 | Parties other than the Subscriber shall not archive the Subscriber Private Key:<br>If the CA or any of its designated RAs generated the Private Key on behalf of the Subscriber, then the CA shall encrypt the Private Key for transport to the Subscriber.<br>If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.<br>(See SSL Baseline Requirements Section 10.2.4) |
| | **Subscriber Agreement and Terms of Use** |
| 3.4 | The CA maintains controls and procedures to provide reasonable assurance that the CA, prior to the issuance of a Certificate, obtains a Subscriber and/or Terms of Use agreement in accordance with the SSL Baseline Requirements Section 10.3.1. That agreement contains provisions imposing obligations and warranties on the Application relating to:<br>- the accuracy of information<br>- protection of Private Key<br>- acceptance of certificate<br>- use of certificate<br>- reporting and revocation<br>- termination of use of certificate<br>- responsiveness<br>- acknowledgement and acceptance.<br>(See SSL Baseline Requirements Section 10.3) |
| 4 | **VERIFICATION PRACTICES** |

| | |
|---|---|
| | **Authorization by Domain Name Registrant** |
| 4.1 | The CA maintains controls and procedures to provide reasonable assurance that as of the date the Certificate was issued, the CA obtains confirmation in accordance with the SSL Baseline Requirements Section 11.1 related to the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate.<br>(SSL Baseline Requirements Section 11.1) |
| | **Verification of Subject Identity Information** |
| 4.2 | 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 SSL Baseline Requirements Section 11.2:<br>• Identity (SSL Baseline Requirements Section 11.2.1)<br>• DBA/Trade name (SSL Baseline Requirements Section 11.2.2)<br>• Authenticity of Certificate Request (SSL Baseline Requirements Section 11.2.3)<br>• Verification of Individual Applicant (SSL Baseline Requirements Section 11.2.4)<br>• Verification of Country (SSL Baseline Requirements Section 11.2.5) |
| 4.3 | The CA maintains controls and procedures to provide reasonable assurance that it inspects any document relied upon for identity confirmation for alteration or falsification.<br>(See SSL Baseline Requirements Section 11.2) |
| 4.4 | The CA maintains controls and procedures to provide reasonable assurance that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA shall not accept any certificate requests that are outside this specification. The CA shall provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.<br>(See SSL Baseline Requirements Section 11.2.3) |
| 4.5 | The CA maintains controls and procedures to provide reasonable assurance that it screens proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located, when the subjectcountryName field is present.<br>(See SSL Baseline Requirements Section 11.2.5) |
| 4.6 | The CA maintains controls and procedures to provide reasonable assurance that the CA does not use any data or document from a source specified under Section 11 of SSL Baseline Requirements to validate a certificate request if the data or document was obtained more than thirty-nine (39) months prior to issuing the Certificate |

| | |
|---|---|
| | (See SSL Baseline Requirements Section 11.3) |
| 4.7 | **The CA maintains controls and procedures 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.<br>(See SSL Baseline Requirements Section 11.4) |
| 4.8 | The CA maintains controls and procedures to provide reasonable assurance that the CA identifies high risk certificate requests, and conduct additional verification activity in accordance with the SSL Baseline Requirements.<br>(See SSL Baseline Requirements Section 11.5) |
| 4.9 | The CA maintains controls and procedures to provide reasonable assurance that, prior to using a data source, the CA evaluates the data source's accuracy and reliability in accordance with the requirements set forth in section 11.6 of the SSL Baseline Requirements. |
| | **Certificate Issuance by a Root CA** |
| 4.10 | **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.<br>(See Baseline Requirements Section 12) |
| 4.11 | **The CA maintains controls to provide reasonable assurance that Root CA Private Keys must not be used to sign Certificates except as permitted by** the Baseline Requirements.<br>(See SSL Baseline Requirements Section 12) |
| 5 | **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 request and related inquiries.<br>(See Baseline Requirements Section 13.1.1) |
| 5.2 | 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; |

| | |
|---|---|
| | • 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 Baseline Requirements Section 13.1.2, 13.1.3 and 13.1.4) |
| 5.3 | The CA maintains controls to provide reasonable assurance that Certificates are revoked within 24 hours if any of the following events 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 SSL Baseline Requirements Section 13.1.5);<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;<br>• 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 SSL Baseline Requirements Section 13.1.5) |

| | |
|---|---|
| 5.4 | The CA maintains controls to provide reasonable assurance that the CA;<br>• makes revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with the Baseline Requirements Appendix B<br>• For high-traffic FQDN, distribute its OCSP responses in accordance with Baseline Requirements.<br><br>(See SSL Baseline Requirements Section 13.2.1) |
| 5.5 | 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.<br>• for the status of Subscriber Certificates<br>o If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven days, and the value of the nextUpdate field must not be more than ten days beyond the value of the thisUpdate field; and<br>o The CA shall update information provided via an Online Certificate Status Protocol (OCSP) at least every four days and OCSP responses must have a maximum expiration time of ten (10) days.<br>• for the status of subordinate CA Certificates<br>o The CA shall update and reissue CRLs at least (i) once every twelve 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<br>o The CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.<br>• effective 1 January 2013, the CA makes revocation information available through the OCSP capability using the GET method for Certificates issued in accordance with these Requirements<br><br>(See Baseline Requirements Section 13.2.2) |
| 5.6 | 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<br><br>(See SSL Baseline Requirements Section 13.2.3) |
| 5.7 | 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.<br><br>(See SSL Baseline Requirements Section 13.2.4) |

| | |
|---|---|
| 5.8 | The CA maintains controls to provide reasonable assurance that OCSP responses conform to RFC2560 and/or RFC5019, and are signed either:<br>• by the CA that issued the Certificates whose revocation status is being checked, or<br>• 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 RFC2560).<br><br>(See SSL Baseline Requirements Section 13.2.5) |
| 5.9 | After the effective date set by the CA/B Forum guidelines, the CA maintains controls to provide reasonable assurance that OCSP responses do not respond with a "good" status for Certificates that have not been issued.<br><br>(See SSL Baseline Requirements Section 13.2.6) |
| 6 | **EMPLOYEE AND THIRD PARTIES** |
| 6.1 | The CA maintains controls to verify the identity and trustworthiness of an employee, agent, or independent contractor prior to engagement of such persons in the Certificate Management Process.<br><br>(See SSL Baseline Requirements Section 14.1.1) |
| 6.2 | The CA maintains controls to provide reasonable assurance that:<br>• the CA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic 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.<br>• 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.<br>• Validation Specialists engaged in Certificate issuance maintains skill levels consistent with the CA's training and performance programs.<br>• the CA documents 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 the Baseline Requirements.<br><br>(See SSL Baseline Requirements Section 14.1.2) |
| 6.3 | The CA maintains controls to provide reasonable assurance that before the CA authorizes |

| | |
|---|---|
| | a Delegated Third Party to perform a delegated function, the CA contractually require the Delegated party to:<br>• meet the qualification requirements of the Baseline Requirements Section 14.1, when applicable to the delegated function;<br>• retain documentation in accordance with the Baseline Requirements Section 15.3.2;<br>• abide by the other provisions of the Baseline Requirements that are applicable to the delegated function; and<br>• comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.<br><br>(See SSL Baseline Requirements Section 14.2.1) |
| 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 and the document retention and event logging requirements of Section 15.<br>(See SSL Baseline Requirements Section 14.2.1) |
| 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.<br>(See SSL Baseline Requirements Section 14.2.1) |
| 6.6 | The CA maintains controls to provide reasonable assurance that the CA internally audits each Delegated Third Party's compliance with the Baseline Requirements on an annual basis.<br>(See SSL Baseline Requirements Section 14.2.2) |
| 6.7 | The CA maintains controls to provide reasonable assurance that the CA does not accept certificate requests authorized by an Enterprise RA unless the Baseline Requirements are met, and the CA imposes these requirements on the Enterprise RA, and monitor compliance by the Enterprise RA.<br>(See SSL Baseline Requirements Section 14.2.4) |
| 7 | **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.<br><br>(See SSL Baseline Requirements Section 15.1) |
| 7.2 | The CA maintains controls to provide reasonable assurance that the following events are recorded:<br><br>• CA key lifecycle management events, including:<br>  ○ key generation, backup, storage, recovery, archival, and destruction<br>  ○ cryptographic device lifecycle management events.<br>• CA and Subscriber Certificate lifecycle management events, including:<br>  ○ Certificate Requests, renewal and re-key requests, and revocation<br>  ○ all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement<br>  ○ date, time, phone number used, persons spoken to, and end results of verification telephone calls<br>  ○ acceptance and rejection of certificate requests<br>  ○ issuance of Certificates<br>  ○ generation of Certificate Revocation Lists (CRLs) and OCSP entries.<br>• security events, including:<br>  ○ successful and unsuccessful PKI system access attempts<br>  ○ PKI and security system actions performed<br>  ○ security profile changes<br>  ○ system crashes, hardware failures, and other anomalies<br>  ○ firewall and router activities<br>  ○ entries to and exits from CA facility.<br>• Log entries must include the following elements:<br>  ○ Date and time of entry<br>  ○ Identity of the person making the journal entry<br>  ○ Description of entry<br><br>(See SSL Baseline Requirements Section 15.2) |
| 7.3 | The CA has a policy and maintains controls to provide reasonable assurance that audit logs generated after the effective date of the Baseline Requirements are retained for at least seven years.<br><br>(See SSL Baseline Requirements Section 15.3.1) |
| 7.4 | The CA has a policy and 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.<br><br>(See SSL Baseline Requirements Section 15.3.2) |

| | |
|---|---|
| 8 | **Audit** |
| 8.1 | The CA maintains controls to provide reasonable assurance that the following requirements are followed for Subordinate CAs:<br>• the Subordinate CA is technically constrained in accordance with SSL Baseline Requirements Section 9.7 and the CA performs the following:<br>  o monitors the Subordinate CA's adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practices Statement; and<br>  o performs quarterly assessments against a randomly selected sample of at least three percent (3%) of the Certificates issued by the Subordinate CA in the period beginning immediately after the last samples was taken to ensure all applicable Baseline Requirements are met; or<br>• for a Subordinate CA that is not technically constrained:<br>  o the CA verifies that Subordinate CAs that are not technically constrained are audited in accordance with SSL Baseline Requirements 17.1.<br><br>(See SSL Baseline Requirements Section 9.7, 17, 17.1 and 17.9) |
| 8.2 | The CA maintains controls to provide reasonable assurance that prior to certificate issuance if the CA uses a non-Enterprise RA Designated Third Party the following requirements are followed:<br>• if the Designated Third Party is not currently audited<br>  o the CA uses an out-of-band mechanism involving at least one human who is acting on either on behalf of the CA or on behalf of the Delegated Third Party to confirm the authenticity of the certificate request or the information supporting the certificate request, or<br>  o the CA performs the domain control validation process itself.<br><br>(See SSL Baseline Requirements Section 17.5 but note that the second bullet is not being considered for audit) |
| 8.3 | The CA maintains controls to provide reasonable assurance that:<br>• it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self-assessment samples was taken,<br>• Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in the Baseline Requirements, the CA performs ongoing quarterly assessments against a randomly selected sample of at least three percent (3%) of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last samples was taken<br>• 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. |

| | |
|---|---|
| | (See SSL Baseline Requirements Section 17.8) |
| 8.4 | 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 SSL certificates.<br><br>(See SSL Baseline Requirements Section 8.1) |

**PRINCIPLE 3: CA Environmental Security -** The Certification Authority maintains effective controls to provide reasonable assurance that:

- Logical and physical access to CA systems and data is restricted to authorized individuals;
- The continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.

| | |
|---|---|
| 1 | The CA develops, implement, and maintain a comprehensive security program designed to:<br>• protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;<br>• protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;<br>• protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;<br>• protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and<br>• comply with all other security requirements applicable to the CA by law.<br><br>(See SSL Baseline Requirements Section 16.1) |
| 2 | The CA performs a risk assessment at least annually that:<br>• Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;<br>• Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and<br>• Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats. (See SSL Baseline Requirements Section 16.2) |
| 3 | The CA develops, implement, and maintain a Security Plan consisting of security procedures, measures, and products designed to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan:<br>• includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes.<br>• takes into account then-available technology and the cost of implementing the specific measures, and<br>• is designed to implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.<br><br>(See SSL Baseline Requirements Section 16.3) |

| | |
|---|---|
| 4 | The CA develops, implement, and maintain a Business Continuity Plan that includes at a minimum:<br>• the conditions for activating the plan;<br>• emergency procedures;<br>• fall-back procedures;<br>• resumption procedures;<br>• a maintenance schedule for the plan;<br>• awareness and education requirements;<br>• the responsibilities of the individuals;<br>• recovery time objective (RTO);<br>• regular testing of contingency plans;<br>• the CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;<br>• a requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;<br>• what constitutes an acceptable system outage and recovery time;<br>• how frequently backup copies of essential business information and software are taken;<br>• the distance of recovery facilities to the CA's main site; and<br>• procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.<br><br>The Business Continuity Plan is tested at least annually, reviewed, and updated.<br><br>(See SSL Baseline Requirements Section 16.4)<br><br>*(For organizations that are undergoing a WebTrust for CA audit (examination), all of the above are required and already tested with the exception of the disclosure of the distance of recovery facilities to the CA's main site.)* |
| 5 | The Certificate Management Process includes:<br>• physical security and environmental controls (see WTCA 2.0 Section 3.4);<br>• system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention (see WTCA 2.0 Section 3.7);<br>• network security and firewall management, including port restrictions and IP address filtering (see WTCA 2.0 Section 3.6);<br>• user management, separate trusted-role assignments, education, awareness, and training (see WTCA 2.0 Section 3.3); and<br>• logical access controls, activity logging, and inactivity time-outs to provide individual accountability (see WTCA 2.0 Section 3.6).<br><br>The CA implements multi-factor authentication for all user accounts capable of directly causing certificate issuance.<br><br>(See SSL Baseline Requirements Section 16.5) |
| 6 | The CA maintains controls to provide reasonable assurance that:<br>• physical access to CA facilities and equipment is limited to authorized individuals, protected |

| | |
|---|---|
| | through restricted security perimeters, and is operated under multiple person (at least dual custody) control;<br>• CA facilities and equipment are protected from environmental hazards;<br>• loss, damage or compromise of assets and interruption to business activities are prevented; and<br>• compromise of information and information processing facilities is prevented.<br><br>(WTCA 2.0 Section 3.4 in support of Section 16.5 of the SSL Baseline Requirements) |
| 7 | The CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.<br><br>(WTCA 2.0 Section 3.7 in support of Section 16.5 of the SSL Baseline Requirements) |
| 8 | The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that:<br>• operating system and database access is limited to authorized individuals with predetermined task privileges;<br>• access to network segments housing CA systems is limited to authorized individuals, applications and services; and<br>• CA application use is limited to authorized individuals.<br><br>Such controls must include, but are not limited to:<br>• network security and firewall management, including port restrictions and IP address filtering;<br>• logical access controls, activity logging (WTCA 2.0 Section 3.10), and inactivity time-outs to provide individual accountability.<br><br>(WTCA 2.0 Section 3.6 in support of Section 16.5 of the SSL Baseline Requirements) |
| 9 | The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.<br><br>(WTCA 2.0 Section 3.3 in support of Section 16.5 of the SSL Baseline Requirements) |
| 10 | The CA maintains controls to provide reasonable assurance that:<br>• significant CA environmental, key management, and certificate management events are accurately and appropriately logged;<br>• the confidentiality and integrity of current and archived audit logs are maintained;<br>• audit logs are completely and confidentially archived in accordance with disclosed business practices; and<br>• audit logs are reviewed periodically by authorized personnel<br><br>(WTCA 2.0 Section 3.10 in support of Section 16.5 of the SSL Baseline Requirements) |

| | |
|---|---|
| 11 | The CA maintains controls to provide reasonable assurance that:<br>• private keys are protected in a system or device that has been validated as meeting at least FIPS 140[-2] level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats;<br>• private keys outside the validated system or device specified above are protected with physical security, encryption, or a combination of both in a manner that prevents disclosure of the private keys;<br>• private keys are encrypted with an algorithm and key-length that meets current strength requirements (2048 bit minimum);<br>• private keys are backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment; and<br>• physical and logical safeguards to prevent unauthorized certificate issuance.<br><br>(See SSL Baseline Requirements Section 16.6) |

**PRINCIPLE 4: Network and Certificate Systems Security Requirements -** The Publicly Trusted Certification Authority maintains effective controls to meet the Network and Certificate System Security Requirements set forth by the CA/Browser Forum.

| | |
|---|---|
| | **General Protections for the Network and Supporting Systems** |
| 1 | The CA maintains controls to provide reasonable assurance that:<br>• Certificate Systems are segmented into networks or zones based on their functional, logical, and physical (including location) relationship;<br>• The same security controls for Certificate Systems apply to all systems co-located in the same zone;<br>• Root CA Systems are located in a High Security Zone and in an offline state or air-gapped from all other networks;<br>• Issuing Systems, Certificate Management Systems, and Security Support Systems are maintained and protected in at least a Secure Zone;<br>• Security Support Systems are implemented and configured to protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks;<br>• Networks are configured with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations;<br>• Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are configured by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party;<br>• Configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies;<br>• Administration access to Certificate Systems are granted only to persons acting in Trusted Roles and receive their accountability for the Certificate System's security;<br>• Multi-factor authentication is implemented to each component of the Certificate System that supports it;<br>• Authentication keys and passwords for any privileged account or service account on a Certificate System is changed, when a person's authorization to administratively access that account on the Certificate System is changed or revoked; and<br>• Recommended security patches are applied to Certificate Systems within six months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.<br><br>(See Network and Certificate Systems Security Requirements Section 1) |
| | **Trusted Roles, Delegate Third Parties, and System Accounts** |
| 2 | The CA maintains controls to provide reasonable assurance that: |

- A documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them is followed;
- The responsibilities and tasks assigned to Trusted Roles are documented and "separation of duties" for such Trusted Roles based on the risk assessment of the functions to be performed is implemented;
- Only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones;
- Individuals in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role;
- Employees and contractors observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems;
- Trusted Role use a unique credential created by or assigned to that person for authentication to Certificate Systems;
- Trusted Role using an username and password to authenticate shall configure accounts to include but not be limited to:
    - Passwords have at least twelve (12) characters for accounts not publicly accessible (accessible only within Secure Zones or High Security Zones);
    - Configure passwords for accounts that are accessible from outside a Secure Zone or High Security Zone to have at least eight (8) characters, be changed at least every 90 days, use a combination of at least numeric and alphabetic characters, and not be one of the user's previous four passwords; and implement account lockout for failed access attempts; OR
    - Implement a documented password management and account lockout policy that the CA has determined provide at least the same amount of protection against password guessing as the foregoing controls.
- Trusted Roles log out of or lock workstations when no longer in use;
- Workstations are configured with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user;
- Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations;
- Revoke account access to Certificate Systems after no more than five (5) failed access attempts, provided that this security measure is supported by the Certificate System and does not weaken the security of this authentication control;
- Disable all privileged access of an individual to Certificate Systems within 24 hours upon termination of the individual's employment or contracting relationship with the CA or Delegated Third Party;
- Enforce multi-factor authentication for administrator access to Issuing Systems and Certificate Management Systems;
- Each Delegated Third Party, shall be:
    - Required to use multi-factor authentication prior to the Delegated Third Party approving issuance of a Certificate; or
    - Be technically constrained that restrict the Delegated Third Party's ability to approve certificate issuance for a limited set of domain names; and
- Restrict remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when:
    - The remote connection originates from a device owned or controlled by the CA or Delegated Third Party and from a pre-approved external IP address,
    - The remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication, and
    - The remote connection is made to a designated intermediary device meeting the following:
        - Located within the CA's network,

| | |
|---|---|
| | ▪ Secured in accordance with these Requirements, and<br>▪ Mediates the remote connection to the Issuing System.<br><br>(See Network and Certificate Systems Security Requirements Section 2) |
| | **Logging, Monitoring and Alerting** |
| 3 | The CA maintains controls to provide reasonable assurance that:<br><br>• Security Support System under the control of CA or Delegated Third Party Trusted Roles are implemented to monitor, detect, and report any security-related configuration change to Certificate Systems;<br>• Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity and are configured to continuously monitor and log system activity;<br>• Automated mechanisms under the control of CA or Delegated Third Party Trusted Roles are configured to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events;<br>• Trusted Role personnel follows up on alerts of possible Critical Security Events;<br>• A human review of application and system logs is performed at least every 30 days and includes:<br>o Validating the integrity of logging processes<br>o Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly; and<br>• Maintain, archive, and retain logs in accordance with disclosed business practices.<br><br>(See Network and Certificate Systems Security Requirements Section 3) |
| | **Vulnerability Detection and Patch Management** |
| 4 | The CA maintains controls to provide reasonable assurance that:<br><br>• Detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles are implemented to protect Certificate Systems against viruses and malicious software;<br>• A formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities;<br>• Perform a Vulnerability Scan on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following:<br>o Within one week of receiving a request from the CA/Browser Forum,<br>o After any system or network changes that the CA determines are significant, and<br>o At least once per quarter;<br>• Perform a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant;<br>• Document that Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test; and |

| | |
|---|---|
| | • Perform one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process:<br>  ○ Remediate the Critical Vulnerability;<br>  ○ If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following:<br>  ▪ Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and<br>  ▪ Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or<br>  ○ Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following:<br>  ▪ The CA disagrees with the NVD rating;<br>  ▪ The identification is a false positive;<br>  ▪ The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or<br>  ▪ Other similar reasons.<br><br>(See Network and Certificate Systems Security Requirements Section 4) |

**Appendix A**

# CA/Browser Forum

# Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.1.6

**and**

# Network and Certificate System Security Requirements v.1.0

To download a copy of the current CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.6 and Network and Certificate System Security Requirements v1.0 go to:

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

## Appendix B

## Sections of Baseline Requirements not subject to audit (examination) under WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

| Baseline Section Ref. | Topic | Reason for exclusion from WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security |
|---|---|---|
| 1 | Scope | No auditable items |
| 2 | Purpose | No auditable items |
| 3 | references | No auditable items |
| 4 | Definitions | No auditable items |
| 5 | Abbreviations and Acronyms | No auditable items |
| 6 | Conventions | No auditable items |
| 7 | Certificate Warranties and Representations | Legal item |
| 14.2.3 | Allocation of liability | Legal item |
| 17.1 | Eligible Audit Schemes | No auditable items |
| 17.2 | Audit period | No auditable items |
| 17.3 | Audit Report | No auditable items |
| 17.4 | Pre-Issuance Readiness audit | No auditable items |
| 17.6 | Auditor Qualifications | No auditable items |
| 18.2 | Indemnification of Application software Suppliers | Legal item |
| 18.3 | Root CA Obligations | Legal item |

## Appendix C

## Sections of the Network and Certificate Systems Security Requirements (NCSR) not subject to audit (examination) under WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

| NCSR Ref. | Topic | Reason for exclusion from WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security |
|---|---|---|
| 2.g.ii | Password controls | Items would require disclosures of user passwords or rainbow table scans of the password hash values. |