# WEBTRUST® FOR CERTIFICATION AUTHORITIES –
SSL BASELINE REQUIREMENTS AUDIT CRITERIA
V.1.0

**BASED ON:**

# CA/BROWSER FORUM

BASELINE REQUIREMENTS
FOR THE ISSUANCE AND MANAGEMENT
OF PUBLICLY-TRUSTED CERTIFICATES, V.1.0

# TABLE OF CONTENTS

This document has been prepared for the use by those auditors recognized as eligible to perform SSL Baseline Requirements audits by the CA/Browser Forum.

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

| **Chair** | **Staff Contact:** |
|---|---|
| Donald E. Sheehy<br>*Deloitte & Touche LLP*<br><br>Michael Greene<br>*Ernst & Young LLP*<br><br>Mark Lundin<br>*KPMG LLP*<br><br>Jeffrey Ward<br>*Stone Carlie & Company LLC* | Bryan Walker,<br>*Canadian Institute of Chartered Accountants* |

The Task Force would like to express its appreciation to the contribution of Mark Lundin who has been a member of the Task Force since its inception. Effective August 1, 2012 Mark was replaced by Reema Anand of KPMG who has been a significant contributor to the WebTrust Certification Authorities program. Mark will continue to advise the Task Force going forward. The Task Force would also like to thank Robert Ikeoka, KPMG LLP for his significant contribution in the preparation of this guide.

# INTRODUCTION

1. The primary goal of the CA/Browser Forum "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, 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.

2. A working group known as the CA/Browser Forum consisting of many of the issuers of digital certificates and browser developers has developed a set of 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, v.1.0 ("SSL Baseline Requirements") can be found at http://www.cabforum.org/.

3. 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 include a specific requirement for CAs that wish to issue SSL certificates.

4. The purpose of these "WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, v.1.0" ("SSL Baseline Audit Criteria") is to set criteria that would be used as a basis for an auditor to conduct a SSL Baseline audit.

***Proposed Adoption***

5. Version 1.0 of the SSL Baseline Requirements is scheduled to become effective July 1, 2012. Version 1.0 of the SSL Baseline Audit Criteria is scheduled to become effective on approval, however earlier implementation to coincide with the effective date of the SSL Baseline Requirements is encouraged.

6. The CA/Browser Forum may periodically publish errata that capture changes to the SSL Baseline Requirements. In addition the CA/Browser Forum will periodically modify the SSL Baseline Requirements to reflect more substantive changes in a point version (e.g., version 1.1). The auditor would need to consider only the updated approved version. The auditor is not required to consider the errata document.

7. As mentioned, the SSL Baseline Audit Criteria are to be used only in conjunction with an audit of the Certification Authority as required by the CA/Browser Forum

[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.

Guidelines. Due to the significant overlaps in the requirements of the SSL Baseline Audit Criteria and WebTrust for CA 2.0, this audit should be conducted simultaneously with the WebTrust for CA 2.0 audit.

8. 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.

9. 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.

10. In preparing the WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria, V1.0, the Task Force reviewed the CA/Browser Forum's Baseline Requirements for the Issuance and Management for Publicly-Trusted Certificates, V1.0 with the intent of identifying those requirements that would not be included in a WebTrust audit. The results of this review are set out in Appendix E.

# CERTIFICATION AUTHORITIES – BASELINE REQUIREMENTS (SSL) AUDIT CRITERIA

**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.

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| 1 | The CA and its Root 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>(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 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 | | |

[2] The criteria are those that are to be tested for the purpose of expressing an opinion on WebTrust for Certificate Authorities - SSL Baseline Requirements Audit Criteria, v.1.0. 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 Guidelines.

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | Baseline Requirements are updated annually.<br><br>(See SSL Baseline Requirements Section 8.2.1) | | |
| 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.<br><br>(See Baseline Requirements 8.2.2) | | |

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

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

| | **Baseline Requirements (SSL) Audit Criteria** | | |
|---|---|---|---|
| | | | |
| | 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 v1.0 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>• Subscriber 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>- Appendix A - Cryptographic Algorithm and Key Requirements<br>- Appendix B - Certificate Extensions.<br>(See SSL Baseline Requirements Section 9) | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| 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 v1.0 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>(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, tradename, 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>(See SSL Baseline Requirements Section 9.2.6) | | |
| 2.4 | The CA maintains controls and procedures to provide reasonable assurance that Certificates are valid for a period not exceeding 60 months.<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). | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| | (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.<br>(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** | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| 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. | | |
| | **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 v1.0 Section 11.2:<br>• Identity (SSL Baseline Requirements Section 11.2.1)<br>• DBA/Tradename (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) | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| | • 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><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><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><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 to validate a certificate request if the data or document was obtained more than thirty-nine (39) months prior to the Certificates' issuance<br><br>(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><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 Baseline Requirements.<br><br>(See SSL Baseline Requirements Section 11.5) | | |
| 4.9 | The CA maintains controls and procedures to provide reasonable assurance that the CA evaluates the data source's accuracy and reliability, and does not use a data source to verify Subject Identity Information if the CA's evaluation | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| | determines that the data source is not reasonably accurate or reliable.<br>(See SSL Baseline Requirements Section 11.6) | | |
| | **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;<br>• identifies high priority Certificate Problem Reports;<br>• begin investigation of Certificate Problem Reports within 24 hours:<br>• decides whether revocation or other appropriate action is warranted; and<br>• where appropriate, forwards such complaints to law enforcement.<br>(See Baseline Requirements Section 13.1.2, Section 13.1.3 and Section 13.1.4) | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| 5.3 | 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>(See SSL Baseline Requirements Section 13.2.1) | | |
| 5.4 | The CA maintains controls to provide reasonable assurance that an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA:<br>• for Subscriber Certificates<br>- CRLs are updated and reissued at least every seven (7) days, and the nextUpdate field value is not more than ten (10) days, or<br>- if the CA provides revocation of information via an Online Certificate Status Protocol (OCSP) service, the OCSP service is updated at least every four (4) days, and OCSP responses from this service must have a maximum expiration time of ten (10) days.<br>• for subordinate CA Certificates<br>- CRLs are updated and reissued at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the nextUpdate field is not more than twelve (12) months; or<br>- if the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, the OCSP service is updated at least every twelve (12) months, and within 24 hours after revoking the 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>(See Baseline Requirements Section 13.2.2) | | |
| 5.5 | 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 | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| | 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) | | |
| 5.6 | 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 | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| | response time of ten seconds or less under normal operating conditions<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>(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>(See SSL Baseline Requirements Section 13.2.5) | | |
| 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>(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 | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| | 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>(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>(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 | 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) | | |
| 6.6 | 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) | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| 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>(See SSL Baseline Requirements Section 15.1) | | |
| 7.2 | The CA maintains controls to provide reasonable assurance that the following events are recorded:<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>-<br>Log entries must include the following elements:<br>- Date and time of entry | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| | - Identity of the person making the journal entry<br>- Description of entry<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>(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>(See SSL Baseline Requirements Section 15.3.2) | | |
| 8 | **AUDIT** | | |
| 8.1 | 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>- 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>- the CA performs the domain control validation process itself.<br>(See SSL Baseline Requirements Section 17.5 but note that the second bullet is not being considered for audit) | | |
| 8.2 | 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 | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | | | |
| | • 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.<br>(See SSL Baseline Requirements Section 17.8) | | |
| 8.3 | 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>(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.

| | **Baseline Requirements (SSL) Audit Criteria** | | |
|---|---|---|---|
| | | | |
| 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>(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 | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | 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>(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>• fallback 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>The Business Continuity Plan is tested at least annually, reviewed, and updated.<br>(See SSL Baseline Requirements Section 16.4)<br>*(For organizations that are undergoing a WebTrust for CA's 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.)* | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| 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>The CA implements multi-factor authentication for all accounts capable of directly causing certificate issuance.<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>(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>(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 | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | individuals, applications and services; and<br>• CA application use is limited to authorized individuals.<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>(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>(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>(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 | | |

| | Baseline Requirements (SSL) Audit Criteria | | |
|---|---|---|---|
| | roles using, at least, dual control in a physically secured environment; and<br>• physical and logical safeguards to prevent unauthorized certificate issuance.<br>(See SSL Baseline Requirements Section 16.6) | | |

**Appendix A**

# CA/BROWSER FORUM

# GUIDELINES FOR
# BASELINE REQUIREMENTS FOR THE ISSUANCE AND MANAGEMENT OF PUBLICLY-TRUSTED CERTIFICATES V1.0

To download a copy of the current CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0 go to:

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

# Appendix B

## Illustrative Practitioners' Reports for WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, v.1.0

### Example 1 –AICPA reporting standards Reporting on Management's Assertion, WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria (Period of Time)

**Report of Independent Accountant**

To the Management of
ABC Certification Authority, Inc.:

We have examined the assertion by the management of ABC Certification Authority, Inc. (ABC-CA) **[hyperlink to management's assertion]** that in providing its SSL Certification Authority (CA) services at LOCATION, ABC-CA, during the period [*date*] through [*date*] it —

- Disclosed its Certificate practices and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- Maintained effective controls to provide reasonable assurance that:
    - The Certificate Policy and/or Certificate Practice Statement are available on a 24x7 basis and updated annually;
    - 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 certificates it manages was established and protected throughout their life cycles;
    - Logical and physical access to CA systems and data was restricted to authorized individuals;
    - The continuity of key and certificate management operations was maintained; and
    - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

for the [*list SSL CAs and roots that are subject to examination*], based on the AICPA/CICA WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria Version 1.0 **[hyperlink to WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria version 1.0]**.

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of ABC-CA's key and SSL certificate life cycle management business practices and its controls over key and SSL certificate integrity, over the continuity of key and certificate life cycle management operations, and over the

development, maintenance, and operation of systems integrity; (2) testing transactions executed in accordance with disclosed key and certificate life cycle management business practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, ABC- CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, for the period [*date*] through [*date*], ABC-CA management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA/CICA WebTrust for Certification Authorities – Baseline Requirements Audit Criteria version 1.0.

This report does not include any representation as to the quality of ABC-CA's certification services beyond those covered by the AICPA/CICA WebTrust for Certification Authorities – Baseline Requirements Audit Criteria version 1.0, nor the suitability of any of ABC-CA's services for any customer's intended purpose

[*For use when a seal is issued*] ABC-CAs use of the WebTrust for Certification Authorities – Baseline Requirements Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

## Example 2 – AICPA reporting standards reporting on Management's Assertion, WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria (Point in Time)

**Report of Independent Practitioner**

To the Management of
ABC Certification Authority, Inc.:

We have examined the assertion by the management of ABC Certification Authority, Inc. (ABC-CA) [hyperlink to management's assertion] that ABC-CA's controls over its Certification Authority (CA) services [Name of Service (at LOCATION, ABC-CA,)] were suitably designed to meet the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria [hyperlink to WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria] as of [*date*]. ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of ABC-CA's key and SSL certificate life cycle management business practices and its controls over key and SSL certificate integrity, over the continuity of key and certificate life cycle management operations, and over the development, maintenance, and operation of systems integrity; (2) evaluating the suitability of the design of the controls; and (3) performing such other procedures as we considered necessary in the circumstances.
In our opinion, ABC-CA management's assertion set forth in the first paragraph, as of [*date*], is fairly stated, in all material respects, based on the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria.

[Management has not placed its Certification Authority (CA) services in operation and, therefore, additional changes to the design of the controls may be made before the CA service is implemented.][3] We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of ABC-CA's controls, individually or in the aggregate.

Because of the nature and inherent limitations of controls, ABC- CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report does not include any representation as to the quality of ABC-CA's certification services beyond those covered by the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, or the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

[3] Pre-implementation only

## Example 3 – CICA reporting standards, Reporting on Management's Assertion, WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria (Period of Time)

**Auditor's Report**

To the Management of
ABC Certification Authority, Inc.:

We have audited the assertion by the management of ABC Certification Authority, Inc. (ABC-CA) [hyperlink to management's assertion] that during the period [*date*] through [*date*] for its Certification Authority (CA) operations at LOCATION, ABC-CA, ABC-CA has:

- Disclosed its Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- Maintained effective controls to provide reasonable assurance that:
  - 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 certificates it manages was established and protected throughout their life cycles.
- Maintained effective controls to provide reasonable assurance that:
- Logical and physical access to CA systems and data was restricted to authorized individuals;
- The continuity of key and certificate management operations was maintained; and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

in accordance with the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria [hyperlink to WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria].

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion based on our audit.

Our audit was conducted in accordance with standards for assurance engagements established by the Canadian Institute of Chartered Accountants (CICA) and, accordingly, included (1) obtaining an understanding of ABC Company's SSL certificate life cycle management practices and procedures, including its relevant controls over the issuance, renewal and revocation of SSL certificates; (2) selectively testing transactions executed in accordance with disclosed SSL certificate life cycle management practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, ABC-CA management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit

Criteria.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, ABC- CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report does not include any representation as to the quality of ABC-CA's certification services beyond those covered by the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, or the suitability of any of ABC-CA's services for any customer's intended purpose.

[*For use when a seal is issued*] ABC Company's use of the WebTrust for SSL Baseline Requirements Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.]

[*Name of CA firm*]
Chartered Accountants
[*City, Province*]
[*Date of report*]

## Example 4 – CICA reporting standards, Reporting on Management's Assertion, WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria (Point in Time)

**Auditor's Report**

To the Management of
ABC Certification Authority, Inc.:

We have audited the assertion by the management of ABC Certification Authority, Inc. (ABC-CA) [hyperlink to management's assertion] that in providing its Certification Authority (CA) services [Name of Service (at LOCATION, ABC-CA,)] as of [*date*], ABC-CA has suitably designed its practices and procedures based on the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria [hyperlink to WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria]. ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion based on our audit.

Our audit was conducted in accordance with standards for assurance engagements established by the Canadian Institute of Chartered Accountants (CICA) and, accordingly, included (1) obtaining an understanding of ABC-CA's SSL certificate life cycle management practices and procedures, including its relevant controls over the issuance, renewal and revocation of SSL certificates; (2) evaluating the suitability of the design of practices and procedures; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, ABC-CA's management's assertion, as of [*date*], is fairly stated, in all material respects, in accordance with the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria.

[Management has not placed its Certification Authority (CA) services in operation and, therefore, additional changes may be made to the design of the controls before the System is implemented.][4] We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of ABC-CA's controls, individually or in the aggregate.

Because of the nature and inherent limitations of controls, ABC- CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report does not include any representation as to the quality of ABC-CA's certification services beyond those covered by the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, or the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Name of CA firm*]
Chartered Accountants
[City, Province]
[Date of report]

[4] Pre-implementation only

## Example 5 – International reporting standards, Reporting on Management's Assertion, WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria (Period of Time)

**Independent Auditor's Report**

To the Management of
ABC Certification Authority, Inc.:

We have examined the assertion by the management of ABC Certification Authority, Inc. (ABC-CA) [hyperlink to management's assertion] that during the period [*date*] through [*date*] for its Certification Authority (CA) operations at LOCATION, ABC-CA, ABC-CA has:

- Disclosed its Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- Maintained effective controls to provide reasonable assurance that:
  - 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 certificates it manages was established and protected throughout their life cycles.
- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

in accordance with the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria [hyperlink to WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria].

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion based on our audit.

Our audit was conducted in accordance with International Standards on Assurance Engagements and, accordingly, included:

(1) obtaining an understanding of ABC-CA's SSL certificate life cycle management practices and procedures, including its relevant controls over the issuance, renewal and revocation of SSL certificates,
(2) selectively testing transactions executed in accordance with disclosed SSL certificate life cycle management practices,
(3) testing and evaluating the operating effectiveness of the controls, and
(4) performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion.

In our opinion, ABC-CA management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors, present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, ABC- CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report does not include any representation as to the quality of ABC-CA's certification services beyond those covered by the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, or the suitability of any of ABC-CA's services for any customer's intended purpose.

[*For use when a seal is issued*] ABC Company's use of the WebTrust for SSL Baseline Requirements Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.]

[Name of firm]
[City, Country]
[Date]

## Example 6 – International standards, Reporting on Management's Assertion, WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria (Point in Time)

**Auditor's Report**

To the Management of
ABC Certification Authority, Inc.:

We have examined the assertion by the management of ABC Certification Authority, Inc. (ABC-CA) [hyperlink to management's assertion] that in providing its Certification Authority (CA) services [Name of Service (at LOCATION, ABC-CA,)] as of [*date*], ABC-CA has suitably designed its practices and procedures based on the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria [hyperlink to WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria]. ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion based on our audit.

Our audit was conducted in accordance with International Standards on Assurance Engagements and, accordingly, included

(1) obtaining an understanding of ABC-CA's SSL certificate life cycle management practices and procedures, including its relevant controls over the issuance, renewal and revocation of SSL certificates,
(2) evaluating the suitability of the design of practices and procedures; and
(3) performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion.

In our opinion, ABC-CA's management's assertion, as of [*date*], is fairly stated, in all material respects, in accordance with the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria.

[Management has not placed its Certification Authority (CA) services in operation and, therefore, additional changes may be made to the design of the controls before the System is implemented.][5] We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of ABC-CA's controls, individually or in the aggregate.

Because of the nature and inherent limitations of controls, ABC- CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report does not include any representation as to the quality of ABC-CA's certification services beyond those covered by the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, or the suitability of any of ABC-CA's services for any customer's intended purpose.

[Name of firm]
[City, Country]
[Date]

[5] Pre-implementation only

# Appendix C

## Illustrative Management Assertions for WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, v.1.0

### Example 1 - Assertion by Management of a Certification Authority, WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria (Period of Time)

**Assertion by Management of ABC Certification Authority, Inc. Regarding Its Disclosure of its Certificate Practices and its Controls Over its SSL Certification Authority Services During the Period [*Date*] through [*Date*]**

[*Date*]

The management of ABC Certification Authority, Inc. (ABC-CA) has assessed the disclosure of its certificate practices and its controls over its SSL - CA services located at LOCATION, ABC-CA for the period [*date*] to [*date*]. Based on that assessment, in ABC-CA Management's opinion, in providing its SSL - CA services at [LOCATION], ABC-CA, during the period from [*date*] through [*date*], ABC-CA:

- Disclosed its Certificate practices and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- Maintained effective controls to provide reasonable assurance that:
    - The Certificate Policy and/or Certificate Practice Statement are available on a 24x7 basis and updated annually;
    - 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 certificates it manages was established and protected throughout their life cycles;
    - Logical and physical access to CA systems and data was restricted to authorized individuals;
    - The continuity of key and certificate management operations was maintained; and
    - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

in accordance with the AICPA/CICA WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria.

[*Name*]

[*Title*]

# Appendix D

## Illustrative Management Representation Letter for WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, v.1.0

### Example 1: - Management Representation Letter for a Certification Authority, All of the Trust Services Criteria for Certification Authorities are Applicable

[Date]

[*Name of CPA or Chartered Accountant firm*]
[*Address*]

Dear Members of the Firm:

Management confirms its understanding that your examination ['audit' in Canada] of our assertion related to ABC Certification Authority, Inc.'s (ABC-CA) business practices disclosure and controls over its SSL Certification Authority operations during the period [*date*], through *date*, was made for the purpose of expressing an opinion on whether our assertion is fairly presented, in all material respects, and that your opinion is based on criteria for effective controls as stated in our assertion document. We are responsible for our assertion. In connection with your examination, management of ABC-CA:

*a.* Acknowledges its responsibility for establishing and maintaining effective controls over its SSL Certification Authority (CA) operations at LOCATION, including CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls.

*b.* Has performed an assessment and believes that ABC-CA's CA SSL business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls met the minimum requirement of the criteria described in our assertion document during the period *date* , through *date* .

*c.* Has disclosed to you that there are no significant deficiencies in the design or operation of the controls which could adversely affect ABC-CA's ability to comply with the control criteria related to ABC-CA's CA SSL business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls, consistent with our assertions.

*d.* Has made available to you all significant information and records related to our assertion.

*e.* Has responded fully to all inquiries made to us by you during your examination.

*f.* Has disclosed to you any changes occurring or planned to occur subsequent to [*date field work ended*], in controls or other factors that might significantly affect the controls, including any corrective actions taken by management with regard to significant deficiencies.

In management's opinion, ABC-CA, in providing its SSL Certification Authority (CA) services at LOCATION, ABC-CA, during the period [*date*] through [*date*], —

- Disclosed its Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- Maintained effective controls to provide reasonable assurance that:
  - 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 certificates it manages was established and protected throughout their life cycles.
- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

for the *[list CAs and roots that are subject to examination*], based on the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria.

Very truly yours,

[*Name*]
[*Title*]

## Appendix E

## Sections of Baseline Requirements not subject to examination (audit) under WebTrust Audit Criteria

| CA/Forum Baseline Section Ref. | Topic | Reason for exclusion from WebTrust SSL Baseline Audit Requirements |
|---|---|---|
| | | |
| 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 |