CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

WebTrust® for Certification Authorities

WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES — SSL BASELINE WITH NETWORK SECURITY

Release Date 31 March 2023

Effective Date For engagement periods commencing on or after 1 April 2023

Based on the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates – Version 1.8.6, and Network and Certificate Systems Security Requirements – Version 1.7

Document History

Version	Publication Date	Revision Summary
2.6	31 January 2022	Updated SSL Baseline Criteria to conform to SSL Baseline Requirements v1.8.0 and Network Security Requirements v1.7. • Principle 2, Criteria 2.17 – additional conditions added. • Principle 2, Criteria 4.6 – removal dates added. • Principle 2, Criteria 5.3 – additional event added and other minor change). • Principle 2, Criteria 7.3 – updated requirements for audit logs. • Principle 4, Criteria 4.3 and 4.6 – conform to updates in Network Security Requirements from v1.4 to v1.7.
2.7	31 January 2023	Updated SSL Baseline Criteria to conform to SSL Baseline Requirements v1.8.6 and Network Security Requirements v1.7. • The Network Security Criteria for Principle 4, when needed, has been separated into a separate document supporting the new WebTrust Principles and Criteria for Certification Authorities – Network Security that was released January 31, 2023. • Principle 2, Criteria 2.12 – updated based on new requirements. • Principle 2, Criteria 4.7 – removed. • Principle 2, Criteria 7.1 and 7.2 and 7.4 – updated based on new requirements. • Principle 2, Criteria 7.5 – new. • Other minor changes throughout.

Acknowledgements

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

Members of the Task Force are:

- Timothy Crawford, *BDO USA, LLP* (co-Chair)
- Dan Adam
- Donoghue Clarke, *Ernst & Young LLP*
- Chris Czajczyc, *Deloitte LLP*
- Adam Fiock, *BDO USA, LLP*
- Eric Lin, *Ernst & Young LLP*
- Zain Shabbir, *KPMG LLP*
- Donald E. Sheehy

CPA Canada Support

- Anna-Marie Christian, Director Emerging Issues & Strategic Partnerships
- Dave Chin, Principal, WebTrust (co-Chair)
- Lilia Dubko, Manager, Assurance Programs

The Task Force would like to thank retiring long-term task force members Jeffrey Ward, *BDO USA, LLP* who also chaired the Task Force since 2016, and David Roque, *Ernst & Young LLP* for their significant contributions to the advancement of the WebTrust program during their membership on the Task Force.

Table of Contents

Introduction

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

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

The Forum has also issued additional security guidelines (the "Network and Certificate System Security Requirements") that apply to all publicly trusted Certification Authorities (CAs), regardless of certificate type being issued.

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

Adoption and effective dates

These Criteria incorporate and make reference to relevant CA/Browser Forum Guidelines and Requirements as listed in Appendix A, and are effective for engagement periods commencing on or after 1 April 2023. Earlier adoption is permitted and encouraged.

The Forum may periodically publish updated Guidelines and Requirements. The practitioner is generally not required to consider these updated versions until reflected in the subsequently updated Criteria. However, in certain circumstances whereby a previous requirement or guidelines is eliminated or made less restrictive, the practitioner may consider those changes as of their effective dates even if the changes are not reflected in the most current Criteria.

In certain instances, the Forum updates its Guidelines and Requirements with certain criteria only effective at a date later than the publication date. The practitioner is directed to review the document history, revisions, and relevant dates in the Forum documents to understand the applicability of certain Guidelines and Requirements.

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

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

Additionally, practitioners should be aware that Browsers may impose additional requirements, above and beyond the CA/Browser Forum Guidelines and Requirements that would be outside of the scope of an engagement performed in accordance with WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security. The practitioner is encouraged to make such enquiries of the CA to determine whether any additional procedures should be performed and related reporting undertaken to satisfy the relevant Browser(s). When such additional procedures are required outside of the scope of the WebTrust criteria specified herein, practitioners should also consider the appropriate reporting to be issued to the Browser(s) to satisfy their requirements.

Connection with WebTrust for CA

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

Requirements not subject to assurance

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

Engagement scoping

Section 5 of the CA/Browser Forum's ("Forum") Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates incorporate the CA/Browser Forum's Network and Certificate System Security Requirements by reference as if fully set forth in the document.

As a result, these SSL Baseline with Network Security criteria incorporate two different CA/Browser Forum requirements documents:

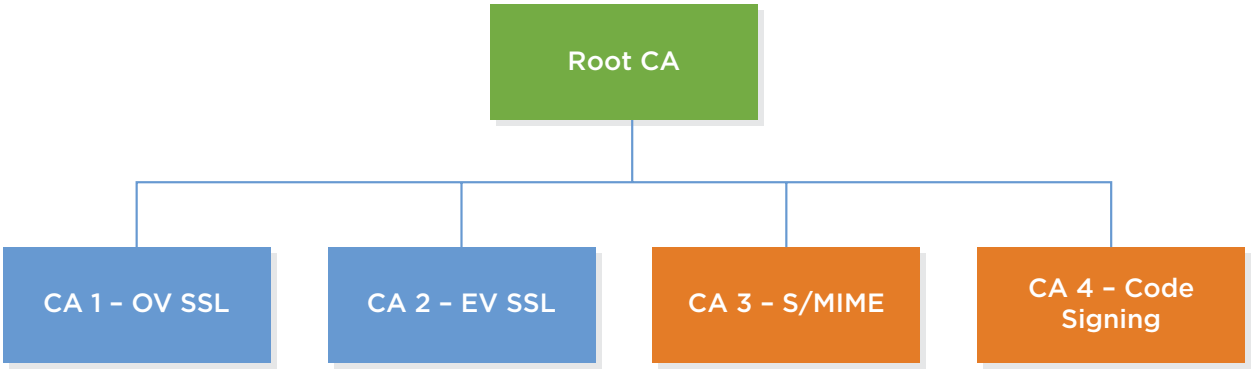
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("SSL Baseline Requirements"); and
- Network and Certificate System Security Requirements ("Network Security Requirements").

The SSL Baseline Requirements are addressed in Principles 1, 2, and 3 of these Criteria. The Network Security Requirements are now referenced in Principle 4 of these Criteria to the WebTrust Principles and Criteria for Certification Authorities – Network Security.

The SSL Baseline Requirements only apply to PKI hierarchies (root and subordinate CAs) that issue or are capable of issuing publicly trusted SSL/TLS certificates intended to authenticate servers on the Internet (i.e. certificates containing the id_kp_serverAuth OID (1.3.6.1.5.5.7.3.1) and/or the anyExtendedKeyUsage OID (2.5.29.37.0) in the extKeyUsage extension).

The Network Security Requirements apply to all CAs within a publicly trusted PKI hierarchy, even if those certificates are designed for other uses (i.e., code signing, client authentication, secure email, document signing etc.).

For example, in the following PKI hierarchy consisting of a Root CA and 4 Subordinate CAs directly underneath it:



The SSL Baseline Requirements (Principles 1, 2, and 3) would only apply to Root CA, CA 1, and CA 2 (provided CA 3 and CA 4 are technically constrained and are not capable of issuing SSL/TLS certificates). However, the Network Security Requirements (Principle 4) would apply to all CAs – Root CA, CA 1, CA 2, CA 3, and CA 4.

The practitioner is directed to consider the above when determining which criteria are in scope for the engagement.

Principle 1: SSL Baseline Requirements Business Practices Disclosure

The Certification Authority (CA) discloses its SSL Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Requirements.

#	Criterion	Ref[2]
1	The CA discloses[3] on its website: • SSL Certificate practices, policies and procedures; • 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 • 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.	2.2, 3.2.6
2	The CA 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.	9.8
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.	7.1.6
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.	2.0, 2.3
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 and include all material required by RFC 3647.	2

2 Reference to the applicable section(s) of the SSL Baseline Requirements for this criterion. The practitioner is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion.

3 The criteria are those in scope for the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security engagement. 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.

#	Criterion	Ref[2]
6	The CA discloses in its Certificate Policy (CP) and/or Certification Practices Statement (CPS) under section 4.2 its policy or practice on processing CAA (Certification Authority Authorisation) DNS Records for Fully Qualified Domain Names that is consistent with the SSL Baseline Requirements, and specifies the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue. The CA maintains controls to provide reasonable assurance that it logs all actions taken, if any, consistent with its processing practice.	2.2
7	The CA's CP/CPS provides a link to a web page or an email address for contacting the person or persons responsible for operation of the CA.	1.5.2
8	The CA has controls to provide reasonable assurance that public access to its repository is read-only.	2.4

Principle 2: SSL Service Integrity

The Certification Authority (CA) 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.

Key generation ceremonies

#	Criterion	Ref[4]
1.1	The CA maintains controls to provide reasonable assurance that Root CA and Subordinate CA Key Pairs are created in accordance with SSL Baseline Requirements Section 6.1.1.1.	6.1.1.1

Certificate content and profile

#	Criterion	Ref[4]
2.1	The CA maintains controls to provide reasonable assurance that Root, Subordinate, and Subscriber certificates generated by the CA contain certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.	7.1
2.2	The CA maintains controls to provide reasonable assurance that the version of certificates issued are of type x.509 v3.	7.1.1
2.3	The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Root CA certificates generated conform to the Baseline Requirements.	7.1.2.1, 6.1.5, 7.1.6, 7.1.6.2
2.4	The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subordinate CA certificates conform to the Baseline Requirements.	7.1.2.2, 6.1.5, 7.1.6, 7.1.6.3

4 Reference to the applicable section(s) of the SSL Baseline Requirements for this criterion. The auditor is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion.

#	Criterion	Ref[4]
2.5	The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subscriber certificates generated conform to the Baseline Requirements.	7.1.2.3, 6.1.5, 7.1.6, 7.1.6.4
2.6	The CA maintains controls to provide reasonable assurance that with exception to the requirements stipulated in the Baseline Requirements Sections 7.1.2.1, 7.1.2.2, and 7.1.2.3, all other fields and extensions of certificates generated are set in accordance with RFC 5280.	7.1.2.4
2.7	The CA maintains controls to provide reasonable assurance that the validity period of Subscriber certificates issued does not exceed the maximum as specified in the Baseline Requirements.	6.3.2
2.8	The CA maintains controls to provide reasonable assurance that it does not issue certificates with extensions that do not apply in the context of the public Internet, unless: a. Such values fall within an OID arc for which the Applicant demonstrates ownership; or b. The Applicant can otherwise demonstrate the right to assert the data in public context.	7.1.2.4
2.9	The CA maintains controls to provide reasonable assurance that it does not issue certificates with semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA.	7.1.2.4
2.10	The CA maintains controls to provide reasonable assurance that it does not issue any new Subscriber or Subordinate CA certificates using the SHA-1 hash algorithm.	7.1.3
2.11	The CA maintains controls to provide reasonable assurance that the content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support a valid Certification Path in accordance with Section 7.1.4.1 of the SSL Baseline Requirements.	7.1.4.1

#	Criterion	Ref[4]
2.12	The CA maintains controls to provide reasonable assurance that for Subscriber certificates issued: • The subjectAltName extension is present and contains at least one entry • Each entry MUST be either: — A dNSName containing the Fully-Qualified Domain Name or Wildcard Domain Name that the CA has validated in accordance with Section 3.2.2.4. Wildcard Domain Names MUST be validated for consistency with Section 3.2.2.6. The entry MUST conform to the requirements of Section 7.1.4.2.1; or — An iPAddress containing an IPv4 or IPv6 address that the CA has validated in accordance with Section 3.2.2.5. The entry MUST NOT contain a Reserved IP Address.	7.1.4.2.1
2.13	The CA maintains controls to provide reasonable assurance that it does not issue certificates containing a Reserved IP Address or Internal Name in the subjectAltName extension or subject:commonName field.	7.1.4.2.1
2.14	The CA maintains controls to provide reasonable assurance that dNSNames in the subjectAltName extension do not contain underscore characters.	7.1.4.2.1
2.15	The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including: • subject:commonName • subject:organizationName • subject:givenName • subject:surname • subject:streetAddress • subject:localityName • subject:stateOrProvinceName • subject:postalCode • subject:countryName • subject:organizationalUnitName • Other Subject Attributes • Subject field requirements if Reserved Certificate Policy Identifiers are asserted • Subject Information for Root and Subordinate CA certificates	7.1.4.2.2, 7.1.6, 7.1.4.3
2.16	The CA maintains controls to provide reasonable assurance that Subordinate CA certificates technically constrained using the nameConstraints extension conform to the Baseline Requirements.	7.1.5

#	Criterion	Ref[4]
2.17	The CA maintains controls to provide reasonable assurance that it rejects a certificate request if one or more of the following conditions are met: • The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6; • There is clear evidence that the specific method used to generate the Private Key was flawed; • The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise; • The CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1; • The CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).	6.1.1.3, 6.1.5, 6.1.6
2.18	The CA maintains controls to provide reasonable assurance that the version numbers and extensions of CRLs conform to the Baseline Requirements.	7.2.2

Certificate request requirements

#	Criterion	Ref[4]
3.1	The CA maintains controls to provide reasonable assurance that the CA, prior to the issuance of a Certificate obtains the following documentation from the Applicant: 1. A certificate request, which may be electronic; 2. An executed Subscriber or Terms of Use Agreement, which may be electronic; and 3. Any additional documentation the CA determines necessary to meet the Baseline Requirements.	4.1.2
3.2	The CA maintains controls to provide reasonable assurance that the Certificate Request is: • obtained and complete prior to the issuance of Certificates; • signed by the appropriate Applicant Representative on behalf of the applicant; • properly certified as to being correct by the applicant; and • contains the information specified in Section 4.2.1 of the SSL Baseline Requirements.	4.1.2, 4.2.1

Subscriber and Subordinate CA Private Keys

#	Criterion	Ref[4]
3.3	The CA maintains controls to provide reasonable assurance that it does not archive the Subscriber or Subordinate CA Private Keys. Additionally: • If the CA or any of its designated RAs generated the Private Key on behalf of the Subscriber or Subordinate CA, then the CA shall encrypt the Private Key for transport to the Subscriber or Subordinate CA. • If the CA or any of its designated RAs become aware that a Subscriber's or Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber or Subordinate CA, then the CA shall revoke all certificates that include the Public Key corresponding to the communicated Private Key. • The CA only archives a Subscriber or Subordinate CA Private Key if it receives authorisation from the Subscriber or Subordinate CA.	6.1.2, 6.2.5, 6.2.6

Subscriber Agreements and Terms of Use

#	Criterion	Ref[4]
3.4	The CA maintains controls 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 9.6.3. That agreement contains provisions imposing obligations and warranties on the Application relating to: • the accuracy of information • protection of Private Key • acceptance of certificate • use of certificate • reporting and revocation • termination of use of certificate • responsiveness • acknowledgement and acceptance.	9.6.3

Verification practices

Verification of Domain Control

#	Criterion	Ref[4]
4.1	The CA maintains controls to provide reasonable assurance that prior to issuing a Certificate: • the CA obtains confirmation in accordance with the SSL Baseline Requirements Sections 3.2.2.4, 3.2.2.5, 3.2.2.6 and 4.2.2 related to the Fully-Qualified Domain Name(s) (including wildcard domains and new gTLDs (generic top-level domains)) and IP address(es) listed in the Certificate; • when the FQDN is an Onion Domain, the CA validates the FQDN in accordance with Appendix B of the SSL Baseline Requirements; and • the CA maintains records of which validation method, including the relevant SSL Baseline Requirements version number, used to validate every domain and IP address.	3.2.2.4, 3.2.2.5, 3.2.2.6, 4.2.2 Appendix B

Verification of Subject Identity Information

#	Criterion	Ref[4]
4.2	The CA maintains controls to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the SSL Baseline Requirements: • Identity (SSL Baseline Requirements Section 3.2.2.1) • DBA/Trade name (SSL Baseline Requirements Section 3.2.2.2) • Authenticity of Certificate Request (SSL Baseline Requirements Section 3.2.5) • Verification of Individual Applicant (SSL Baseline Requirements Section 3.2.3) • Verification of Country (SSL Baseline Requirements Section 3.2.2.3)	3.2.2.1, 3.2.2.2, 3.2.5, 3.2.3, 3.2.2.3
4.3	The CA maintains controls to provide reasonable assurance that it inspects any document relied upon for identity confirmation for alteration or falsification.	3.2.2

#	Criterion	Ref[4]
4.4	The CA maintains controls to provide reasonable assurance that it 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.	3.2.5
4.5	The CA maintains controls 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.	3.2.2.3
4.6	The CA maintains controls to provide reasonable assurance that the CA does not use any data or document from a source specified under Section 3.2 of SSL Baseline Requirements to validate a certificate request, or re-use a previously completed validation conducted by itself, if the data or document was obtained, or validation completed more than 825 days prior to issuing the certificate. And: • Validations completed using methods specified in Section 3.2.2.4.1 or Section 3.2.2.4.5 are not re-used on or after 1 August 2018. • Validations completed using the methods specified in Sections 3.2.2.4.9 and 3.2.2.5.4 are not re-used on or after 1 August 2019. • Validations completed using method specified in Section 3.2.2.4.6 are not permitted. Information and validations for domains validated prior can be re-used per applicable certificate data reuse periods.	4.2.1
4.7	Reserved for future use.	
4.8	The CA maintains controls to provide reasonable assurance that the CA identifies high risk certificate requests and conducts additional verification activities in accordance with the SSL Baseline Requirements.	4.2.1
4.9	The CA maintains controls 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 3.2.2.7 of the SSL Baseline Requirements.	3.2.2.7
4.10	The CA maintains controls to provide reasonable assurance that as part of the issuance process, it checks for CAA (Certificate Authority Authorisation) records, and, if present, processes these records and issues certificates in accordance with the requirements set forth in Section 3.2.2.8 of the SSL Baseline Requirements.	3.2.2.8

#	Criterion	Ref[4]
4.11	The CA maintains controls to provide reasonable assurance that it documents potential certificate issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/Browser Forum on the circumstances.	3.2.2.8

Certificate Issuance by a Root CA

#	Criterion	Ref[4]
4.12	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.	4.3.1
4.13	The CA maintains controls to provide reasonable assurance that Root CA Private Keys are not used to sign certificates, except as stipulated in the Baseline Requirements.	6.1.7

Certificate revocation and status checking

#	Criterion	Ref[4]
5.1	The CA maintains controls to provide reasonable assurance that a process is available 24x7 that the CA is able to accept and respond to revocation requests and Certificate Problem Requests, and that the CA provides a process for Subscribers to request revocation of their own certificates.	4.9.3

#	Criterion	Ref[4]
5.2	The CA maintains controls to provide reasonable assurance that it: • has the capability to accept and acknowledge Certificate Problem Reports on a 24x7 basis; • identifies high priority Certificate Problem Reports; • begin investigation of Certificate Problem Reports within 24 hours and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report; • decides whether revocation or other appropriate action is warranted; • if revocation is deemed the appropriate action, the elapsed time from receipt of the Certificate Problem Report or revocation request and revocation status information does not exceed the timelines in SSL Baseline Requirements 4.9.1.1; and • where appropriate, forwards such complaints to law enforcement.	4.9.3, 4.9.5, 4.10.2
5.3	The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or 4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); 5. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon. And, Subscriber Certificates are revoked within 5 days if any of the following events occurs: 1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6; 2. The CA obtains evidence that the Certificate was misused; 3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use; 4. 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);	4.9.1.1, 6.1.5, 6.1.6

#	Criterion	Ref[4]
5.3	*(continued)* 5. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; 6. The CA is made aware of a material change in the information contained in the Certificate; 7. 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; 8. The CA determines that any of the information appearing in the Certificate is inaccurate; 9. 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; 10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or 11. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.	
5.4	The CA maintains controls to provide reasonable assurance that Subordinate CA Certificates are revoked within 7 days if any of the following events occurs: 1. The Subordinate CA requests revocation in writing; 2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6; 4. The Issuing CA obtains evidence that the Certificate was misused; 5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with these Baseline Requirements or the applicable Certificate Policy or Certification Practice Statement; 6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; 8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or 9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.	4.9.1.2, 6.1.5, 6.1.6

#	Criterion	Ref[4]
5.5	• The CA maintains controls to provide reasonable assurance that the CA makes revocation information available via the cRLDistributionPoints and/or authorityInformationAccess certificate extensions for Subordinate CA and Subscriber Certificates in accordance with the SSL Baseline Requirements Section 7.1.2.	7.1.2, 4.9.11
5.6	The CA maintains controls to provide reasonable assurance that an online 24x7 Repository is provided that application software can use to automatically check the current status of all unexpired Certificates issued by the CA, and: • for the status of Subscriber Certificates: — If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven (7) days, and the value of the nextUpdate field must not be more than ten (10) days beyond the value of the thisUpdate field; and — the OCSP responses: • have a validity interval greater than or equal to eight hours; • have a validity less than or equal to ten days; • with validity intervals less than sixteen hours, then the CA SHALL update the information provided via an OCSP prior to one-half of the validity period before the nextUpdate; and • with validity intervals greater than or equal to sixteen hours, the CA SHALL update the information provided via an OCSP at least eight (8) hours prior to the nextUpdate, and no later than four days after the thisUpdate. • for the status of subordinate CA Certificates — The CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field; and — The CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate. • The CA makes revocation information available through an OCSP capability using the GET method for Certificates issued in accordance with the SSL Baseline Requirements.	4.10.2, 4.9.7, 4.9.10
5.7	The CA maintains controls to provide reasonable assurance that the CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.	4.10.2

#	Criterion	Ref[4]
5.8	The CA maintains controls to provide reasonable assurance that the CA does not remove revocation entries on a CRL or OCSP Response until after the Expiry Date of the revoked Certificate.	4.10.1
5.9	The CA maintains controls to provide reasonable assurance that OCSP responses conform to RFC6960 and/or RFC5019, and are signed either: • by the CA that issued the Certificates whose revocation status is being checked, or • by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked (the OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960).	4.9.9
5.10	The CA maintains controls to provide reasonable assurance that OCSP responses by CA's which have not been technically constrained in accordance with SSL Baseline Requirements Section 7.1.5 do not respond with a "good" status for Certificates that have not been issued.	4.9.10

Employees and third parties

#	Criterion	Ref[4]
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.	5.3.1
6.2	The CA maintains controls to provide reasonable assurance that: • the CA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. • the CA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. • the CA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. • the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements. • all personnel in Trusted Roles maintain skill levels consistent with the CA's training and performance programs.	5.3.3, 5.3.4

#	Criterion	Ref[4]
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: • meet the qualification requirements of the Baseline Requirements Section 5.3.1, when applicable to the delegated function; • retain documentation in accordance with the Baseline Requirements Section 5.5.2; • abide by the other provisions of the Baseline Requirements that are applicable to the delegated function; and • 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.	1.3.2, 5.3.1, 5.5.2
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 5.3.3 and the document retention and event logging requirements of Section 5.4.1.	5.3.7, 5.3.3, 5.4.1
6.5	For High Risk Certificate Requests, the CA maintains controls to provide reasonable assurance that the CA verifies that the Delegated Third Party's processes to identify and further verify High Risk Certificate Requests meets the requirements of the CA's own processes for High Risk Certificate Requests.	4.2.1
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.	8.7
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 requirements in SSL Baseline Requirements Section 1.3.2 are met, and the CA imposes these requirements on the Enterprise RA, and monitors compliance by the Enterprise RA.	1.3.2

Data records

#	Criterion	Ref[4]
7.1	The CA maintains controls to provide reasonable assurance that the CA and each Delegated Third Party record events related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; recording events related to their 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.	5.4.1
7.2	The CA maintains controls to provide reasonable assurance that the following events are recorded: • CA certificate and key lifecycle events, including: — Key generation, backup, storage, recovery, archival, and destruction; — Certificate requests, renewal, and re-key requests, and revocation; — Approval and rejection of certificate requests; — Cryptographic device lifecycle management events; — Generation of Certificate Revocation Lists and OCSP entries; — Signing of OCSP Responses (as described in Section 4.9 and Section 4.10); and — Introduction of new Certificate Profiles and retirement of existing Certificate	5.4.1, 4.9, 4.10

#	Criterion	Ref[4]
7.2	*(continued)* • Profiles.Subscriber Certificate lifecycle management events, including: — Certificate Requests, renewal and re-key requests, and revocation; — all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement; — Approval and rejection of certificate requests; — Issuance of Certificates; and — Generation of Certificate Revocation Lists; and — Signing of OCSP entries Responses (as described in Section 4.9 and Section 4.10). • security events, including: — successful and unsuccessful PKI system access attempts; — PKI and security system actions performed; — security profile changes; — Installation, update and removal of software on a Certificate System; — system crashes, hardware failures, and other anomalies; — firewall and router activities; — entries to and exits from CA facility. • Log entries must include the following elements: — Date and time of event — Identity of the person making the journal entry — Description of event	5.4.1, 4.9, 4.10
7.3	The CA maintains controls to provide reasonable assurance that the CA and each Delegated Third Party's audit logs generated are retained for at least two years: 1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of: a. the destruction of the CA Private Key; or b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key; 2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 (2)) after the revocation or expiration of the Subscriber Certificate; 3. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.	5.4.3

#	Criterion	Ref[4]
7.4	The CA maintains controls to provide reasonable assurance that: • Archived audit logs (as set forth in Section 5.5.1) are retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer. • The CA and each delegated party SHALL retain, for at least two (2) years: — All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in Section 5.5.1); and — All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of: • such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or • the expiration of the Subscriber Certificates relying upon such records and documentation.	5.5.1, 5.5.2, 5.4.3
7.5	The CA maintains controls to provide reasonable assurance that the CA and each Delegated Third Party archives all audit logs (as set forth in Section 5.4.1) and also archives: • Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and • Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.	5.5.1, 5.4.1

Audit

#	Criterion	Ref[4]
8.1	The CA maintains controls to provide reasonable assurance that for Subordinate CAs that are considered technically constrained in accordance with SSL Baseline Requirements Section 7.1.5, the CA: • monitors the Subordinate CA's adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practices Statement; and • 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 were taken to ensure all applicable Baseline Requirements are met.	8.1, 8.7, 7.1.5
8.2	The CA maintains controls to provide reasonable assurance that for Subordinate CAs that are NOT considered technically constrained in accordance with SSL Baseline Requirements Section 7.1.5, the CA verifies that Subordinate CAs that are not technically constrained are audited in accordance with SSL Baseline Requirements 8.4.	8.1, 8.4, 7.1.5
8.3	Reserved for future use	
8.4	The CA maintains controls to provide reasonable assurance that: • It performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self-assessment sample was taken; • 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 sample was taken; • 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.	8.7
8.5	The CA maintains controls to provide reasonable assurance that it complies with: • laws applicable to its business and the certificates it issues in each jurisdiction where it operates, and • licensing requirements in each jurisdiction where it issues SSL certificates.	8.0

Principle 3: CA Environmental Security

The Certification Authority (CA) 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.

#	Criterion	Ref[5]
1	The CA maintains controls to provide reasonable assurance that it develops, implements, and maintains a comprehensive security program designed to: • protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes; • protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes; • protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes; • protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and • comply with all other security requirements applicable to the CA by law.	5.0
2	The CA maintains controls to provide reasonable assurance that it performs a risk assessment at least annually which: • 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; • Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and • Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.	5.0, 5.4.8

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

#	Criterion	Ref[5]
3	The CA maintains controls to provide reasonable assurance that it develops, implements, and maintains 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: • includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes; • takes into account then-available technology and the cost of implementing the specific measures; and • 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.	5.0
4	The CA maintains controls to provide reasonable assurance that it develops, implements, and maintains a Business Continuity Plan that includes at a minimum: • the conditions for activating the plan; • emergency procedures; • fall-back procedures; • resumption procedures; • a maintenance schedule for the plan; • awareness and education requirements; • the responsibilities of the individuals; • recovery time objective (RTO); • regular testing of contingency plans; • 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; • a requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • what constitutes an acceptable system outage and recovery time; • how frequently backup copies of essential business information and software are taken; • the distance of recovery facilities to the CA's main site; and • 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. The Business Continuity Plan is tested at least annually, reviewed, and updated.[6]	5.7.1

6 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.

#	Criterion	Ref[5]
5	The CA maintains controls to provide reasonable assurance that its Certificate Management Process includes: • physical security and environmental controls (see WTCA 2.2.2 Section 3.4); • system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/ prevention (see WTCA 2.2.2 Section 3.7); • network security and firewall management, including port restrictions and IP address filtering (see WTCA 2.2.2 Section 3.6); • user management, separate trusted-role assignments, education, awareness, and training (see WTCA 2.2.2 Section 3.3); and • logical access controls, activity logging, and inactivity time-outs to provide individual accountability (see WTCA 2.2.2 Section 3.6).	5.0
6	The CA maintains controls to provide reasonable assurance that: • 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; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented.	5.0 (WTCA v2.2.2 Sec 3.4)
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.	5.0 (WTCA v2.2.2 Sec 3.7)
8	The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that: • operating system and database access is limited to authorized individuals with predetermined task privileges; • access to network segments housing CA systems is limited to authorized individuals, applications and services; and • CA application use is limited to authorized individuals. Such controls must include, but are not limited to: • network security and firewall management, including port restrictions and IP address filtering; • logical access controls, activity logging (WTCA 2.2.2 Section 3.10), and inactivity time-outs to provide individual accountability.	5.0 (WTCA v2.0 Sec 3.6)

#	Criterion	Ref[5]
9	The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	5.0 (WTCA v2.2.2 Sec 3.3)
10	The CA maintains controls to provide reasonable assurance that: • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and • audit logs are reviewed periodically by authorized personnel.	5.0 (WTCA v2.2.2 Sec 3.10)
11	The CA maintains controls to provide reasonable assurance that: • CA 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; • CA 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; • CA private keys are encrypted with an algorithm and key-length that meets current strength requirements (2048-bit minimum); • CA 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 • physical and logical safeguards to prevent unauthorized certificate issuance.	5.2.2, 6.2, 6.2.7
12	The CA maintains controls to provide reasonable assurance that it enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.	6.5.1

Principle 4: Network and Certificate System Security Requirements

The Certification Authority (CA) maintains effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

For Criteria needed to satisfy this Principle, refer to WebTrust Principles and Criteria for Certification Authorities – Network Security.

Appendix A: CA/Browser Forum Documents

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

Document Name	Version	Effective Date
Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	1.8.6	14 December 2022
Network and Certificate System Security Requirements	1.7	5 April 2021

Appendix B: Sections of SSL Baseline Requirements not subject to assurance

Sections of the Baseline Requirements which contain no content or the phrase "No Stipulation" were not considered. Additionally, the following items are not subject to assurance:

Ref	Topic	Reasons for exclusion
1.1	Overview	Information only
1.2	Document Name and Identification	Information only
1.3 (except 1.3.2)	PKI Participants	Information only
1.4	Certificate Usage	Information only
1.5 (except 1.5.2)	Policy Administration	Information only
1.6	Definitions and Acronyms	The practitioner is directed to consider these definitions when interpreting the SSL Baseline Requirements and these criteria.
4.9.2	Who Can Request Revocation	Information only
8.2	Identity/Qualifications of Assessor	Information only
8.6	Communication of Results	Information only
9.6.1	CA Representations and Warranties	Legal item
9.9.1	Indemnification by CAs	Legal item
9.16.3	Severability	Legal item

Appendix C: Sections of Network and Certificate System Security Requirements not subject to assurance

Not applicable at this time.

Appendix D: CA/Browser Forum effective date differences

SSL Baseline Requirements

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

No differences in this version.