CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

WebTrust® for Certification Authorities

WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES – NETWORK SECURITY

Release Date 31 October 2025

Effective Date For engagement periods commencing on or after November 1, 2025

Based on the CA/Browser Forum Baseline Requirements Network and Certificate Systems Security Requirements – Version 2.0.5

Document History

Version	Publication Date	Revision Summary
1.0	31 May 2023	Initial version created based on a separation of Network and Certificate Systems Security Requirements vs 1.7 from version 2.6 of WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security to allow for separate reporting where desired.
1.7	31 March 2024	Minor changes.
2.0.5	31 October 2025	Restructuring of NCSSRs. Changes and additions throughout based on the revisions from version 2.0 and beyond to the NSRs.

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, PC* (co-Chair)
- Chris Czajczyc, *Deloitte LLP*
- Péter Máté Erdősi, *Crowe FST (Hungary)*
- Adam Fiock, *BDO USA, PC*
- Brian Hsiung, *Sun Rise CPA (Taiwan)*
- David Lachmansingh, *Richter LLP*
- Eric Lin, *Ernst & Young LLP*
- Zain Shabbir, *KPMG LLP*
- Masatoshi Shigaki, *KPMG AZSA LLC (Japan)*
- Jinhwan Shin, *Deloitte LLP (Korea)*
- Jeffrey Ward, *Aprio LLP*

CPA Canada Support

- Taryn Abate, Director, Research & Thought Leadership
- Lilia Dubko, Senior Manager, Assurance Programs (co-Chair)
- Jacquelyn Fortuna, Product Coordinator

Table of Contents

Introduction

The primary goal of the CA/Browser Forum's ("Forum") Network and Certificate System Security Requirements ("Network and Certificate System Security Requirements") v2.0.5 is based on an expectation "CAs are expected to maintain a very high level of security for their infrastructure and systems because the certificates they issue play a vital role in the security of the internet, email, and software distribution." One of the outcomes is that "Audit and assessment bodies are able to accurately map these Requirements to the specific implementations observed during audit engagements, and judge compliance against these Requirements." The Requirements also serve to inform users and help them make informed decisions when relying on Certificates.

The CA/Browser Forum, which consists of many of the issuers of digital certificates and browser and other application developers, has developed security guidelines (the "Network and Certificate System Security Requirements") that apply to all publicly trusted Certification Authorities (CAs), regardless of the certificate type being issued.

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

Definitions

Refer to CA/Browser Forum's Network and Certificate Systems Security Requirements, version 2.0.5 for all referenced terms not explicitly defined in this document.

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 November 12, 2025, or after. 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 guideline 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.

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 C.

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 – 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 the significant overlap between these Criteria and the WebTrust Principles and Criteria for Certification Authorities Version 2.2.2 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.

Engagement scoping

As of the time of publication, these Network Security Criteria incorporate Version 2.0.5 of the CA/Browser Forum Network and Certificate System Security Requirements ("Network Security Requirements"). These Network Security Requirements apply to all CAs under a publicly trusted root CA, despite the use, such as TLS, code signing, client authentication, secure email, or document signing. All CAs are to comply with the CA/Browser forum's Network and Certificate Systems Security Requirements (NCSSR). The NCSSRs have been removed from the frameworks for third-party assurance providers related to SSL Baseline, Registration Authority, VMCR, S/MIME and Code Signing, and can be found as these standalone set of Principles and Criteria. For engagement periods commencing on or after November 12, 2025, it is recommended reporting for the NCSSRs be provided under a separate cover from the frameworks for third-party assurance providers related to MCR, EV SSL, SSL Baseline, S/MIME, Code Signing, and Registration Authority Principles and Criteria.

Security Principle 1: CA Infrastructure and Network Boundary Control Configuration

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 CA Infrastructure and Network Boundary Control Configuration.

#	Criterion	Ref[1]
	Network Segmentation	
1	The CA defines and maintains an inventory of its CA Infrastructure.	1
1.1.1	The CA maintains controls to provide reasonable assurance that CA Infrastructure is segmented into separate networks based on the functional and/or logical relationships of CA Infrastructure components.	1.1.1
1.1.1.2	The CA maintains controls to provide reasonable assurance that network segmentation is designed and implemented using Network Boundary Controls, such as: • firewalls; • network switches; • physically separate networks; and • software-defined networking.	1.1.1.2
	CA Infrastructure Security	
1.2.1.1	The CA maintains controls to provide reasonable assurance that CA Infrastructure is located in a Physically Secure Environment.	1.2.1
1.2.1.2	The CA maintains controls to provide reasonable assurance that Root CA Systems are physically separated from all other CA infrastructure.	1.2.1
1.2.2.1	The CA maintains controls to provide reasonable assurance that connections to the CA Infrastructure are authenticated and encrypted, except where a formal specification prohibits or limits the use of authentication and/or encryption.	1.2.2

1 Reference to the applicable section(s) of the Network and Certificate System Security Requirements v2

#	Criterion	Ref[1]
1.2.2.2	The CA maintains controls to provide reasonable assurance that CA Infrastructure and Network Boundary Controls be implemented and configured in a manner that minimizes unnecessary active components and capabilities such that: • all connections, communications, applications, services, protocols, and ports not used are removed and/or disabled; and • only connections, communications, applications, services, protocols, and ports necessary and approved under the Principle of Least Privilege are enabled.	1.2.2
1.2.3	The CA maintains controls to provide reasonable assurance that equivalent security is implemented on all systems on the same network as any CA Infrastructure component.	1.2.3
	Change Management	
1.3.1	The CA maintains controls to provide reasonable assurance that the CA establishes and maintains a change management process that is: 1. documented; 2. authoritative for: — all personnel in Trusted Roles; — management of Network Boundary Controls; and — management of CA Infrastructure; 3. reviewed annually; 4. updated as needed; and 5. approved; — with each update; — prior to going into effect; and — by personnel in applicable Trusted Roles.	1.3

#	Criterion	Ref[1]
1.3.2	The CA maintains controls to provide reasonable assurance that the change management process: 1. enables identification, documentation, remediation of risks associated with introducing, modifying, or removing: — Trusted Roles definitions; — Trusted Roles appointments; — Network Boundary Controls; or — CA Infrastructure. 2. Addresses management exceptions and responding to emergencies; and 3. Incorporates procedures for change reversal where applicable.	1.3
1.3.3	The CA maintains controls to provide reasonable assurance that all changes are completed in accordance with such a change management process for: 1. Trusted Roles definitions; 2. Trusted Roles appointments; 3. Network Boundary Controls; and 4. CA Infrastructure.	1.3

Security Principle 2: Access Control

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 Access Control.

#	Criterion	Ref[1]
	Trusted Roles	
2.1	The CA maintains controls to provide reasonable assurance that it defines Trusted Roles for the personnel who design, build, develop, implement, operate, and maintain its Certificate Systems and Root CA Systems. Each Trusted Role's responsibilities, privileges, and access is documented, and is assigned in a manner consistent with: 1. the Principle of Least Privilege; and 2. the Principle of Separation of Duties.	2.1
2.1.1	The CA maintains controls to provide reasonable assurance that personnel assigned to a Trusted Role act only within the scope of their Trusted Role(s) when performing responsibilities, using privileges, or using access assigned to that Trusted Role.	2.1.1
	Access Management	
2.2.1	The CA maintains controls to provide reasonable assurance that access to Certificate Systems and Root CA Systems is: 1. limited to personnel assigned to applicable Trusted Roles; and 2. based on the Principle of Least Privilege.	2.2.1
2.2.1.1	The CA maintains controls to provide reasonable assurance that personnel assigned to Trusted Roles that are authorized to access or authenticate to Certificate Systems or Root CA Systems use unique authentication credentials created by or assigned to the authorized individual.	2.2.1.1
2.2.1.2	If group accounts or shared role credentials to access CA Infrastructure and/or Network Boundary Controls are used, the CA must be able to attribute each use to: 1. an approved activity; and 2. an individual user or service account.	2.2.1.2

#	Criterion	Ref[1]
2.2.1.3.1	The CA maintains controls to provide reasonable assurance that authentication credentials are changed or revoked when associated authorizations are changed or revoked.	2.2.1.3
2.2.1.3.2	The CA maintains controls to provide reasonable assurance that access to CA Infrastructure and Network Boundary Controls is disabled for personnel within twenty-four (24) hours of the termination of an individual's employment or contracting relationship.	2.2.1.3
2.2.1.4.1	The CA maintains controls to provide reasonable assurance that any account capable of authenticating to or accessing CA Infrastructure or Network Boundary Control is reviewed at a minimum frequency of every three (3) months.	2.2.1.4
2.2.1.4.2	The CA maintains controls to provide reasonable assurance that any account that is not necessary for the operation of CA Infrastructure or Network Boundary Controls is deactivated or removed such that the account is no longer capable of authenticating to or accessing CA Infrastructure or Network Boundary Controls.	2.2.1.4
2.2.1.5	The CA maintains controls to provide reasonable assurance that security measures are implemented that minimize the susceptibility of CA Infrastructure and Network Boundary Controls to unauthorized access through repeated attempts to authenticate to or access an account that has access to CA Infrastructure or Network Boundary Controls.	2.2.1.5
2.2.2	The CA maintains controls to provide reasonable assurance that prevents continued access to the Workstations after a set period of inactivity, for example by automatically logging off active users. The allowed and configured duration of inactivity must be selected based on the CA's assessment of associated risks.	2.2.2
2.2.3	The CA maintains controls to provide reasonable assurance that the CA enforces the use of multi-factor authentication for access to CA Infrastructure. Authentication based on the possession of a cryptographic key may not be used as part of Multi-factor Authentication, unless the key is stored in a key storage device that is designed to prevent extraction.	2.2.3
2.2.4	The CA maintains controls to provide reasonable assurance that it enforces the use of Multi-Party Control for physical access to any Root CA System.	2.2.4

#	Criterion	Ref[1]
2.2.5	The CA maintains controls to provide reasonable assurance that access to shared credentials: 1. be limited to personnel based on the Principle of Least Privilege; and 2. be able to attribute each use to approved activity and an individual user or service account.	2.2.5, 2.2.1.2
2.2.6	The CA maintains controls to provide reasonable assurance that any remote connection that enables Privileged Access to CA Infrastructure: 1. originates from a Workstation owned and/or controlled by the CA; 2. is made through a temporary, non-persistent, and encrypted channel; 3. is authenticated using Multi-Factor Authentication; and 4. is made to a Network Boundary Control asset which: — is located within the CA's network; — is secured in accordance with these Requirements; and — mediates the remote connection to the CA Infrastructure.	2.2.6

Security Principle 3: Network and Certificate System Security Requirements – Monitoring, Logging, Auditing and Incident Response

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 Monitoring, Logging, Auditing and Incident Response.

#	Criterion	Ref[1]
	Monitoring and Logging	
3.1.1	The CA maintains controls to provide reasonable assurance that it identifies and documents the monitoring and logging capabilities of CA Infrastructure and Network Boundary Controls.	3.1.1
3.1.1.1	The CA maintains controls to provide reasonable assurance that the monitoring and logging capabilities of CA Infrastructure and Network Boundary Controls are enabled to the extent necessary to meet: 1. the Network and Certificate System Security Requirements; and 2. applicable obligations that depend on such audit logs (such as the requirements in Section 5.4.1 (3) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates).	3.1.1.1
3.1.1.2	The CA maintains controls to provide reasonable assurance that audit logs produced by the monitoring and logging capabilities of CA Infrastructure and Network Boundary Controls include activities and/or events: 1. necessary to detect possible: — Critical Security Events; and — modifications to CA Infrastructure not authorized through the change management process outlined in Section 1.3 of the Network and Certificate System Security Requirements; and 2. with sufficient detail to meet: — these Network and Certificate System Security Requirements; and — applicable obligations that depend on such audit logs (such as the requirements in Section 5.4.1 (3) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates).	3.1.1.2

#	Criterion	Ref[1]
3.1.2.1	The CA maintains controls to provide reasonable assurance that the integrity of logging processes within CA Infrastructure is monitored through: 1. continuous automated monitoring operating within CA Infrastructure; or 2. a review by personnel assigned to applicable Trusted Roles at least once every 31 days.	3.1.2
3.1.2.2	The CA maintains controls to provide reasonable assurance that integrity monitoring is configured and managed in a manner sufficiently effective to identify possible audit log compromise.	3.1.2
3.1.2.3	The CA maintains controls to provide reasonable assurance that audit logs are retained and/or archived for the amount of time necessary to meet: 1. the Network and Certificate System Security Requirements; and 2. applicable obligations which depend on such audit logs (such as the requirements in Section 5.4.1 (3) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates).	3.1.2.1
	Audit Log Processing and Alerting	
3.2.1	The CA maintains controls to provide reasonable assurance that audit logs are processed: 1. through automated mechanisms under the control of personnel assigned to applicable Trusted Roles; and 2. in a manner sufficiently effective to minimally identify possible: — Critical Security Events; and — unauthorized changes to CA Infrastructure.	3.2.1
3.2.2	The CA maintains controls to provide reasonable assurance that personnel assigned to applicable Trusted Roles are alerted via multiple mechanisms and/or communication channels of identified possible: 1. audit log compromise; 2. Critical Security Events; and 3. unauthorized changes to CA Infrastructure.	3.2.2

#	Criterion	Ref[1]
3.2.3	The CA maintains controls to provide reasonable assurance that personnel assigned to applicable Trusted Roles commence an initial response to alerts of Section 3.2.2 of the Network and Certificate System Security Requirements within twenty-four (24) hours of the alert being generated.	3.2.3
3.2.3.1.1	The CA maintains controls to provide reasonable assurance that the initial response to alerts of Section 3.2.2 of the Network and Certificate Systems Security Requirements confirms whether the alert identifies a legitimate: 1. audit log compromise; 2. Critical Security Event; and/or 3. unauthorized change to the CA Infrastructure.	3.2.3.1
3.2.3.1.2	The CA maintains controls to provide reasonable assurance that personnel assigned to applicable Trusted Roles create and follow an incident response plan for all legitimate alerts.	3.2.3.1

Security Principle 4: Network and Certificate System Security Requirements – Vulnerability Management

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 vulnerability management.

#	Criterion	Ref[1]
4.1.1	The CA maintains controls to provide reasonable assurance that the CA implements the policies and procedures for identifying, evaluating and resolving security vulnerabilities, as required in Section 4 of the Network and Certificate Security Requirements and these policies and procedures must apply to all Certificate Systems.	4
4.1.2	The CA maintains controls to provide reasonable assurance that, effective April 15, 2026, the Network and Certificate System Security Requirements policy and procedures apply to Security Support Systems and Network Boundary Controls.	4
4.1.3	The CA maintains controls to provide reasonable assurance that the CA protects the system in the inventory of CA Infrastructure against common network and system threat using intrusion detection and prevention controls.	4.1
4.2	The CA maintains controls to provide reasonable assurance that it documents and follows a vulnerability correction process that includes: 1. identification; 2. review; 3. response; and 4. remediation.	4.2
4.2.1	The CA maintains controls to provide reasonable assurance that the CA's vulnerability identification process includes monitoring for relevant security advisories and penetration testing.	4.2.1

#	Criterion	Ref[1]
4.2.1.1	The CA maintains controls to provide reasonable assurance that the CA's vulnerability identification and correction process defines and follows a program for performing penetration tests that ensures: 1. penetration tests are performed: — at least on an annual basis; and — after infrastructure or application changes that are organizationally defined as significant; and 2. penetration tests are performed by a person or entity (or collective group thereof) with the requisite skills, tools, proficiency, code of ethics, and independence; and 3. vulnerabilities identified during the penetration test are remediated using the vulnerability correction process in Section 4.2 of the Network and Certificate System Security Requirements.	4.2.1.1
4.2.2	The CA maintains controls to provide reasonable assurance that a vulnerability is determined remediated when the CA has: • fixed the vulnerability such that the vulnerability is no longer present; or • confirmed the impact of the vulnerability and documented why the vulnerability does not impact the CA's security posture.	4.2.2
4.3.1	The CA maintains controls to provide reasonable assurance that the CA establishes one or more timeframes for reviewing, responding to, and remediating all identified vulnerabilities and the timeframes are based on a Risk Assessment performed by the CA. Vulnerabilities are reviewed, responded to, and remediated in accordance with the established timeframes.	4.3
4.3.2	The CA maintains controls to provide reasonable assurance that the Risk Assessment is based on a documented security analysis. The security analysis should take into account and address the following principles: • criticality of assets; • maintaining confidentiality, integrity, and availability of assets; • regulatory requirements; • likelihood and impact of exploitation; • dependencies and interdependencies; • remediation resource requirements; • historical data; and • present threat landscape.	4.3

#	Criterion	Ref[1]
4.3.3	The CA maintains controls to provide reasonable assurance that the CA documents in Section 6.7 of its Certificate Policy and/or Certification Practices Statement each timeframe for responding to and remediating vulnerabilities.	4.3

Appendix A: CA/Browser Forum Documents

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

Document Name	Version	Effective Date
Network and Certificate System Security Requirements Subsections include additional effective dates Section 1 – 3 Section 4	2.0.5	3 July 2025 12 November 2025 15 April 2026

Appendix B: Sections of Network and Certificate System Security Reuirements not subject to assurance

Not applicable at this time.

Appendix C: CA/Browser Forum effective date differences

Network and Certificate System Security Requirements

No differences in this version.