CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

WebTrust® for Certification Authorities

WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES – NETWORK SECURITY

Release Date 31 May 2023

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

Based on the CA/Browser Forum Baseline Requirements Network and Certificate Systems Security Requirements – Version 1.7

VERSION 1.0

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.

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)
- Daniel J. 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
- David 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

Document History ii

Acknowledgements iii

Introduction 1

Adoption and effective dates 1

Connection with WebTrust for CA 2

Requirements not subject to assurance 2

Engagement scoping 2

Security Principle 1: Network and Certificate System Security Requirements – General Protections for Network and Supporting Systems 3

Security Principle 2: Network and Certificate System Security Requirements – Trusted Roles, Delegated Third Parties and Systems Accounts 5

Security Principle 3: Network and Certificate System Security Requirements – Logging, Monitoring, and Alerting 8

Security Principle 4: Network and Certificate System Security Requirements – Vulnerability Detection and Patch Management 10

Appendix A: CA/Browser Forum Documents 12

Appendix B: Sections of Network and Certificate System Security Requirements not subject to assurance 13

Appendix C: CA/Browser Forum effective date differences 14

Network Security Requirements 14

Introduction

The primary goal of the CA/Browser Forum's ("Forum") 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 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 – 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.

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 July 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.

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 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.

Engagement scoping

As of the time of publication, these Network Security criteria incorporate the following 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.

Security Principle 1: Network and Certificate System Security Requirements – General Protections for Network and Supporting Systems

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 General Network and Supporting Systems.

#	Criterion	Ref[1]
1.1	The CA maintains controls to provide reasonable assurance that certificate Systems are segmented into networks based on their functional, or logical relationship.	1.a
1.2	The CA maintains controls to provide reasonable assurance that equivalent security controls are applied to all systems co-located within the same network as a Certificate System.	1.b
1.3	The CA maintains controls to provide reasonable assurance that Root CA Systems are located in a High Security Zone and in an offline state or air-gapped from all other networks.	1.c
1.4	The CA maintains controls to provide reasonable assurance that Issuing Systems, Certificate Management Systems, and Security Support Systems are maintained and protected in at least a Secure Zone.	1.d
1.5	The CA maintains controls to provide reasonable assurance that Security Support Systems are implemented and configured to protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks.	1.e
1.6	The CA maintains controls to provide reasonable assurance that networks are configured with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations.	1.f

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

#	Criterion	Ref[1]
1.7	The CA maintains controls to provide reasonable assurance that Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are configured by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party.	1.g
1.8	The CA maintains controls to provide reasonable assurance that CA's security policies encompass a change management process, following the principles of documentation, approval and review, and to ensure that all changes to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems follow said change management process.	1.h
1.9	The CA maintains controls to provide reasonable assurance that administration access to Certificate Systems is granted only to persons acting in Trusted Roles and require their accountability for the Certificate System's security.	1.i
1.10	The CA maintains controls to provide reasonable assurance that Multi-Factor Authentication is implemented to each component of the Certificate System that supports Multi-Factor Authentication.	1.j
1.11	The CA maintain controls to provide reasonable assurance that authentication keys and passwords for any privileged account or service account on a Certificate System are changed, when a person's authorization to administratively access that account on the Certificate System is changed or revoked.	1.k
1.12	The CA maintains controls to provide reasonable assurance that recommended security patches are applied to Certificate Systems within six (6) months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.	1.l

Security Principle 2: Network and Certificate System Security Requirements – Trusted Roles, Delegated Third Parties and Systems Accounts

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 Trusted Roles, Delegated Third Parties and Systems Accounts.

#	Criterion	Ref[1]
2.1	The CA maintains controls to provide reasonable assurance that a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them is followed.	2.a
2.2	The CA maintains controls to provide reasonable assurance that the responsibilities and tasks assigned to Trusted Roles are documented and "separation of duties" for such Trusted Roles based on the risk assessment of the functions to be performed is implemented.	2.b
2.3	The CA maintains controls to provide reasonable assurance that only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones.	2.c
2.4	The CA maintains controls to provide reasonable assurance that individuals in a Trusted Role act only within the scope of such role when performing administrative tasks assigned to that role.	2.d
2.5	The CA maintains controls to provide reasonable assurance that employees and contractors observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems.	2.e
2.6	The CA maintains controls to provide reasonable assurance that Trusted Roles use a unique credential created by or assigned to that person for authentication to Certificate Systems, and group accounts or shared role credentials are not used.	2.f

#	Criterion	Ref[1]
2.7	The CA maintains controls to provide reasonable assurance that Trusted Roles using a username and password to authenticate shall configure accounts to include but not be limited to: • For accounts accessible only within Secure Zones or High Security Zones: — Passwords have at least twelve (12) characters • For authentications which cross a zone boundary into a Secure Zone or High Security Zone: — Require Multi-Factor Authentication • For accounts accessible from outside a Secure Zone or High Security Zone: — Passwords to have at least eight (8) characters, not be one of the user's previous four (4) passwords; and implement account lockout for failed access attempts in accordance with requirement 2.k (Criterion 2.11); • Routine password changes are completed no more frequently than once every two years.	2.g
2.8	The CA maintains controls to provide reasonable assurance that it has a policy for Trusted Roles to log out of or lock workstations when no longer in use.	2.h
2.9	The CA maintains controls to provide reasonable assurance that it has a procedure to configure workstations with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user, and that workstations are configured in accordance with the policy.	2.i
2.10	The CA maintains controls to provide reasonable assurance that it reviews all system accounts at least every three (3) months and deactivates any accounts that are no longer necessary for operations.	2.j
2.11	The CA maintains controls to provide reasonable assurance that it locks account access to Certificate Systems after no more than five (5) failed access attempts, provided that: • This security measure is supported by the Certificate System; • Cannot be leveraged for a denial-of-service attack and; • Does not weaken the security of this authentication control.	2.k

#	Criterion	Ref
2.12	The CA maintains controls to provide reasonable assurance that it disables all privileged access of an individual to Certificate Systems within twenty-four (24) hours upon termination of the individual's employment or contracting relationship with the CA or Delegated Third Party.	2.l
2.13	The CA maintains controls to provide reasonable assurance that it enforces Multi-Factor Authentication OR multi-party authentication for administrator access to Issuing Systems and Certificate Management Systems.	2.m
2.14	The CA maintains controls to provide reasonable assurance that it enforces Multi-Factor Authentication for all Trusted Role accounts for both itself and Delegated Third Parties on Certificate Systems (including those approving the issuance of a Certificate) that are accessible from outside a Secure Zone or High Security Zone.	2.n
2.15	The CA maintains controls to provide reasonable assurance that it restricts remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when: • The remote connection originates from a device owned or controlled by the CA or Delegated Third Party; • The remote connection is through a temporary, non-persistent encrypted channel that is supported by Multi-Factor Authentication; and • The remote connection is made to a designated intermediary device meeting the following: — Located within the CA's network; — Secured in accordance with the Network and Certificate System Security Requirements; and — Mediates the remote connection to the Issuing System.	2.o

Security Principle 3: Network and Certificate System Security Requirements – Logging, Monitoring, and Alerting

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 Logging, Monitoring and Alerting.

#	Criterion	Ref[1]
3.1	The CA maintains controls to provide reasonable assurance that Security Support Systems under the control of CA or Delegated Third Party Trusted Roles are implemented to monitor, detect, and report any security-related configuration change to Certificate Systems.	3.a
3.2	The CA maintains controls to provide reasonable assurance that Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity are configured to continuously monitor and log system activity in accordance with Section 5.4.1 (3) of the Baseline Requirements.	3.b
3.3	The CA maintains controls to provide reasonable assurance that Automated mechanisms under the control of CA or Delegated Third Party Trusted Roles are configured to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events.	3.c
3.4	The CA maintains controls to provide reasonable assurance that Trusted Role personnel follows up on alerts of possible Critical Security Events.	3.d
3.5	The CA maintains controls to provide reasonable assurance that it monitors the integrity of the logging processes for application and system logs through continuous automated monitoring and alerting or through a human review to ensure that logging and log-integrity functions are effective. Alternatively, if a human review is utilized and the system is online, the process must be performed at least once every 31 days.	3.e

#	Criterion	Ref
3.6	The CA maintains controls to provide reasonable assurance that it monitors the archival and retention of logs to ensure that logs are retained for the appropriate amount of time in accordance with the disclosed business practices and applicable legislation.	3.f
3.7	The CA maintains controls to provide reasonable assurance that If continuous automated monitoring and alerting is utilised to satisfy Network Security Requirements 1.h. or 3.e. that it responds to the alert and initiates a plan of action within at most twenty-four (24) hours.	3.g

Security Principle 4: Network and Certificate System Security Requirements – Vulnerability Detection and Patch 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 detection and patch management.

#	Criterion	Ref[1]
4.1	The CA maintains controls to provide reasonable assurance that intrusion detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles are implemented to protect Certificate Systems against common network and system threats.	4.a
4.2	The CA maintains controls to provide reasonable assurance that a formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities.	4.b
4.3	The CA maintains controls to provide reasonable assurance that a Vulnerability Scan is performed on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following: • Within one (1) week of receiving a request from the CA/Browser Forum; • After any system or network changes that the CA determines are significant; and • At least every three (3) months.	4.c
4.4	The CA maintains controls to provide reasonable assurance that a Penetration Test is performed on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant.	4.d
4.5	The CA maintains controls to provide reasonable assurance that it documents that Vulnerability Scans and Penetrations Tests were performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.	4.e

#	Criterion	Ref[1]
4.6	The CA maintains controls to provide reasonable assurance that it performs one of the following within ninety-six (96) hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: • Remediate the Critical Vulnerability; • If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: — Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and — Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or • Document the factual basis for the CA's determination that the vulnerability does not require remediation because: — The CA disagrees with the NVD rating; — The identification is a false positive; — The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or — Other similar reasons.	4.f

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	1.7	5 April 2021

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

Not applicable at this time.

Appendix C: CA/Browser Forum effective date differences

Network Security Requirements

No differences in this version.