CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

CA/Browser Forum Seattle 63 WebTrust for CA Update

Tim Crawford, Lilia Dubko, Rosemary McGuire

October 2024

Agenda

- CPA Canada Updates
  1. CPA Canada WebTrust Team/Task Force Members
  2. Historical Reports
  3. Website Access
  4. Engagement Applicability Matrix
  5. CA/B Forum F2F meeting #65 in Toronto, Canada
- WebTrust Product Update
  1. Updated Principles and Criteria
  2. Updated Reporting Guidance
- Presenting Cross Signed CA Certificates
- Network Security Considerations
  1. Definitions Updates
  2. Version of NSRs in BRs
- WebTrust Reporting Options

CPA Canada WebTrust Team

Lilia Dubko, Senior Manager

Jacquelyn Fortuna, Product Coordinator

Taryn Abate, Director

Rosemary McGuire, Vice President

Task Force Members

CPA Canada

Lilia Dubko (Co-Chair)

Taryn Abate, Director

Task Force Members

Tim Crawford, BDO (Co-Chair)

Chris Czajczyc, Deloitte

Eric Lin, EY

Adam Fiock, BDO

Zain Shabbir, KPMG

Dan Adam

David Lachmansingh, Richter LLP

Jinhwan Shin, Deloitte

Historical Reports

In response to Browsers’ request to have access to historical WebTrust reports (expired seals), CPA Canada has added functionality to provide links to the historical reports.

Historical reports links from two prior years were made available through CPA Canada portal in September 2024.

Updates to the file will be made on a bi-monthly basis.

Only reports with seals (unqualified or qualified) will be publicly available.

Website Access

During the last F2F meeting, Certification Authorities expressed interest in having access to WebTrust illustrative reports.

Reports can be made available through CPA Canada portal.

CPA Canada requires contact information (Name/Last name, email address and CA company name) to provide access.

Engagement Applicability Matrix

Engagement Applicability Matrix to be updated to include:

- Changes in terminology (e.g., Verified Mark Certificates to Mark Certificates, SSL to TLS, etc.)
- New versions of the Principles and Criteria, effective dates

CA/B Forum F2F meeting #65

CPA Canada will be hosting CA/B Forum F2F meeting #65 in Toronto, Canada, on June 10-12, 2025.

Criteria Updates

Planned Updates

November/December 2024

- WebTrust for CA
- WebTrust for Network Security

April 2025

- WebTrust for SSL Baseline
- WebTrust for Code Signing
- WebTrust S/MIME
- WebTrust for EV
- WebTrust for VMC
- WebTrust for RA

Revised Reporting Templates Coming

Reporting Template Updates VS 3.0

- Templates for reporting on NSRs combined and separate
- Inclusive subservice provider examples
- Management assertion by service provider
- Qualified seal updates
- Updated Canadian and International reports for transitional issues
- Updates to WebTrust for RA
- Example Carve out report
- Other minor updates

Reporting Cross Signed Certificates

Options

CA certificates can be presented on:

1. On the report of the signee
2. On the report of the signor
3. On both reports

Requirements

At a minimum, the Browsers require the cross signed certificate on the report of the signor.

Recommendation

Auditor prefer to include on both reports and indicate on signors report a separate entity controls private key.

Network Security Issues of Note

1. Updates taking effect in November include potential expansion of scope of control responsibilities.

2. Different baseline requirements require different versions of the Network Security and Certificate System requirements.

3. CPA Canada is working to implement NS-004 and NS-005 into December 2024 update of the principles and criteria.

Network Security Definitions – Version 2.0

CA Infrastructure

Collectively the infrastructure used by the CA or Delegated Third Party which qualifies as a:

- Certificate Management System;
- Certificate System;
- Delegated Third Party System;
- Issuing System;
- Root CA System (Air-Gapped and otherwise); or.
- Security Support System.

Security Support System

A system or set of systems supporting the security of the CA Infrastructure, which minimally includes:

1. authentication;
2. network boundary control;
3. audit logging;
4. audit log reduction and analysis;
5. vulnerability scanning;
6. physical intrusion detection;
7. host-based intrusion detection; and.
8. network-based intrusion detection.

Network Security Definitions

Definitions lead to potential expansion of scope

Enterprise infrastructure team supporting:

1. Firewalls or other boundary devices
2. Network directory and authentication systems
3. Teams supporting event management tools

Third party considerations

1. Penetration and vulnerability scanning services
2. Host log repositories

Review the scope with your auditor!

Network Security Versions in the BRs

NSR References in the Baseline Requirements.

TLS Server Certificates – reference version 1.7

Code Signing Certificates – reference version 1.7

S/MIME Certificates – reference version 2.0

We understand there are considerations each set of BRs must accept a new version of the NSRs.

WebTrust Reporting Options

- **Short form**
  - Opinion letter
  - Assertion letter
  - Appendix for CA scoping tables/other content
  - Often around 20 pages

- **Long form/detailed controls report (similar to a SOC 1 or 2 report)**
  - Opinion letter
  - Assertion letter
  - System description
  - Tables of controls, testing procedures, and results
  - Reports approach or exceed 200 pages

WebTrust Reporting Options

Potential additional reporting option (similar to a SOC 3 report)

- Opinion letter
- Assertion letter
- Description of system boundaries
- Appendix for CA scoping tables/other content
- No control details or testing
- Planned to be used for carve out reports to detail controls under the responsibility of carved out project
- Expected length around 30 to 40 pages

WebTrust Reporting Options

Description of System Boundaries (5-10 pages)

- Company background
- Brief overview of services provided
- Overview of components of the system
  - Infrastructure
  - Software
  - People
  - Processes and Procedures
  - Data
- Complimentary subservice organization controls and user entity responsibilities (if applicable)

Thank you! Questions?