CHARTERED PROFESSIONAL ACCOUNTANTS CANADA
COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

CA/Browser Forum Meeting

WebTrust for CA Update

November 7, 2019

Jeff Ward & Don Sheehy

Agenda

- “WETSI”
- Current Status Of Updated WebTrust Documents
- Reporting Requirements and Sample Reports
- Current Status Of Other WebTrust Task Force Projects
- Detailed Controls Reporting
- Reporting Terminology
- Brief CPA Canada Update

“WETSI” - CONTINUING DISCUSSIONS

WETSI

- Attendance at New York meeting September 2019
- Terminology – moving to common language
- Continuing issues faced
- Potential for working together

Current Status of Updated WebTrust Documents

WebTrust for CA 2.2

- Effective for periods beginning on or after June 1, 2019
- Minor updates made to conform to ISO 21188:2018 Edition

WebTrust for Extended Validation vs 1.6.8

- Effective for periods beginning on or after June 1, 2019
- Principle 1, Criteria 4 – RFC 3647 requirement with the sunsetting of 2527
- Principle 2, Criteria 5.2-5.4 – updated revocation requirements based on changes to BRs

Current Status of Updated WebTrust Documents

WebTrust Baseline + NS vs 2.4.1

- Effective for audit periods beginning on or after June 1, 2019.
- Version 2.4.1 of WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – replacing versions 2.3. and 2.4
- Principle 2, Criterion 2.14 corrected for a typographical error
- Principle 4, Criterion 1.2 edited for clarity

Current Status of Updated WebTrust Documents

WebTrust for RA vs 1.0

- Effective for periods beginning on or after April 30, 2019
- Provides a framework for third party assurance providers to assess the adequacy and effectiveness of the controls employed by a Registration Authority (RA) that performs either a portion or all of the registration related functions for a Certification Authority (CA) on an outsourced basis.
- Audit guidance for registration functions that are conducted directly by the CAs entirely are covered in the document, WebTrustSM/TM Principles and Criteria for Certification Authorities.

No changes made to WebTrust for Extended Validation Code Signing, or Publicly Trusted Code Signing

Next round of updates to take place in January 2020

Reporting Requirements and Sample Reports

- Search on cpacanada/webtrust for link to CPA Canada materials
- Reporting requirements are illustrated on matrix at https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria
  - This has been updated to June 2019 releases
- Sample reports have been developed under each standard since W4CA program began – current versions are at https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/practitioner-qualification-and-guidance
  - Additional reports developed to be posted soon

WebTrust Reports Available – Full Lifecycle

- Rootkey Generation Ceremony Report (Birth Certificate)
- Key Protection (Provides assurance that once a key is created and up to the point it is moved into production, it was properly safeguarded)
- Point In Time (As of date for testing the design and implementation of controls)
- Period of Time (Same as Point in Time, but also tests transactions over a period between 2-12 months to ensure controls are operating effectively)
- Key Transportation, Migration & Destruction

Other WebTrust Program Components

Last Updated: 30-June-19											
	RKGC[7]	Key Protection[8]	CA	EV SSL	SSL Baseline + Network	EV CS	CS Publicly Trusted	Additional Microsoft	Additional Mozilla	Additional FPKI	RA
Private PKI	Optional	Optional	Optional	N/A	Optional	N/A	Optional[1]	See footnote 3	N/A	N/A	See footnote 9
Publicly-Trusted Commercial PKI - SSL	Required	Required	Required	N/A	Required	N/A	N/A	See footnote 3	N/A	N/A	See footnote 9
Publicly-Trusted Commercial PKI - EV SSL	Required	Required	Required	Required	Required	N/A	N/A	See footnote 3	N/A	N/A	See footnote 9
Publicly-Trusted Commercial PKI - CS	Required	Required	Required	N/A	Not Required	N/A	Required[1]	See footnote 3	N/A	N/A	See footnote 9
Publicly-Trusted Commercial PKI - EV CS	Required	Required	Required	N/A	Not Required	Required	Required[1]	See footnote 3	N/A	N/A	See footnote 9
Publicly-Trusted Commercial PKI - All other uses	Required	Required	Required	N/A	Not Required	N/A	N/A	See footnote 3	N/A	N/A	See footnote 9
Publicly-Trusted Government PKI - SSL	Required	Required	Required[2]	N/A	Required[2]	N/A	N/A	See footnote 3	See footnote 4	N/A	See footnote 9
Publicly-Trusted Government PKI - EV SSL	Required	Required	Required[2]	Required[2]	Required[2]	N/A	N/A	See footnote 3	See footnote 4	N/A	See footnote 9
Publicly-Trusted Government PKI - CS	Required	Required	Required[2]	N/A	Not Required	N/A	Required[1,2]	See footnote 3	See footnote 4	N/A	See footnote 9
Publicly-Trusted Government PKI - EV CS	Required	Required	Required[2]	N/A	Not Required	Required[2]	Required[1,2]	See footnote 3	See footnote 4	N/A	See footnote 9
Publicly-Trusted Government PKI - All other uses	Required	Required	Required[2]	N/A	Not Required	N/A	N/A	See footnote 3	See footnote 4	N/A	See footnote 9
PKI X-Cert with USA Federal Bridge	Required	Required	Required[5]	N/A	N/A	N/A	N/A	See footnote 3	N/A	See footnote 6	See footnote 9

Footnotes

1 Issuance and Management of Publicly-Trusted Code Signing Certificates is required for periods starting on or after February 1, 2017 for code signing certificates trusted by Microsoft Windows. Refer to http://aka.ms/auditreqs. See section 3.14.

2 Microsoft accepts an 'equivalent' audit for Government CAs in lieu of a WebTrust audit, with certain restrictions. For more information, refer to http://aka.ms/auditreqs.

3 Microsoft publishes specific technical requirements for Roots and certificates that are part of its root programme. Refer http://aka.ms/auditreqs for the most up to date version of the technical requirements.

4 Mozilla does not currently make a distinction between Commercial and Government CAs. Therefore, the requirements for Commercial CAs apply equally to a Government CA if part of the Mozilla Root Programme.

5 Includes special reporting requirements for the Federal PKI

6 Specific CP and CPS disclosures required; must map to CP of Federal Bridge

7 RKGC refers to audit reports to be issued in conjunction with a WebTrust Auditor's witnessing of CA's Root Key Generation Ceremony.

8 Key Protection refers to audit reports to be issued in conjunction with a WebTrust Auditor's witnessing of the migration, transportation or destruction of a CA's Root or Sub CA.

9 WebTrust for Registration Authorities (RA) can be performed by any entity that performs outsourced RA activities. This report may also be required as part of the contractual obligations by the CA, or by an oversight body such as the CA / Browser Forum.

Other WebTrust Program Components

Audit Scheme Versions				
Scheme	Version		Release Date	Effective Date
WebTrust for CA	2.1		01-Sep-17	01-Jul-11
WebTrust for CA	2.2		01-Jun-19	01-Jun-19
WebTrust for CA - Extended Validation - SSL	1.6.2		01-Oct-17	01-Oct-17
WebTrust for CA - Extended Validation - SSL	1.6.8		01-Jun-19	01-Jun-19
WebTrust for CA - Extended Validation - Code Signing	1.4		31-Jan-17	01-Jan-17
WebTrust for CA - Extended Validation - Code Signing	1.4.1		1-Ocr-17	01-Oct-17
WebTrust for CA - SSL Baseline with Network Security	2.2		31-Jan-17	01-Dec-16
WebTrust for CA - SSL Baseline with Network Security	2.3		01-Feb-18	01-Feb-18
WebTrust for CA - SSL Baseline with Network Security	2.4		01-Jun-19	01-Jun-19
WebTrust for CA - SSL Baseline with Network Security	2.4.1		30-Jun-19	01-Jun-19
WebTrust for CA - Publicly Trusted Code Signing Certificates	1.0		01-Feb-17	01-Feb-17
WebTrust for CA - Publicly Trusted Code Signing Certificates	1.0.1		01-Oct-17	01-Oct-17
WebTrust for RA	1.0		30-Apr-19	30-Apr-19

Current Status of Other WTF Projects

Practitioner guidance for auditors

- Under development covering public and private CAs
- Version that combines US, Canada and International
- Provides examples of tools and approaches as best practices
- Latest draft reviewed September 2019 meeting – expected release early 2020

Detailed Control Reporting

- **Shell has been developed - A period of time report has been developed – point in time report does not have a section 4**
  - Section 1- Overall audit results (opinion)
  - Section 2- Management assertion
  - Section 3- Description criteria (includes system description)
  - Section 4- Detailed testing performed and results thereof
  - Section 5 – Unaudited Management comments
- **In essence, asking for reports that have detail similar to a AICPA SOC 2 report (SOC 2 reports issued on restricted distribution basis by audit profession for service organizations)**
- **Expected completion late 2019**

Detailed Control Reporting

- **Is not the primary report**
- **Short form (current report) will be public facing report with seal**
- **Looking for volunteers to review and comment**

Section 1 – Audit report

Summary

- About 5 pages long for US version
- Reporting on disclosure requirements (similar to description criteria) for CA system and suitability of design and effectiveness of controls over the reporting period
- Sets out management and auditor responsibilities
- Sets out inherent limitations
- References tests of controls
- Provides opinion
- Describes the restricted use of the report (those knowledgeable regarding the subject matter)

Section 2 – Management Assertion

Summary

- Developed using WebTrust for CA and SOC 2
- Required for all engagements
- Certain components are required to be included, but management has flexibility to add other information in its assertion

Section 3 – System Description

Summary

- Information that is contained in CP/CPS will not be detailed in the System Description – rather it will have general reference
- Based on comparison of RFC 3647, SOC 2 and SOC for Cyber
- Compared draft requirements to SOC 3 reports on PKI

Disclosure Requirements (New Feature)

- DR1: The nature of the entity's business and operations, including the principal products or services the entity sells or provides and the methods by which they are distributed
- DR 2: The components of the system to provide the services, including the following:
  a. Infrastructure b. Software c. People d. Procedures e. Data
- DR 3: For identified system incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements, as of the date of the description (for a type 1) or during the period of time covered by the description (for a type 2), as applicable, the following information
  a. Nature of each incident
  b. Timing surrounding the incident
  c. Extent (or effect) of the incident and its disposition

Disclosure Requirements (continued)

- DR 4: Any specific applicable trust services criterion that is not relevant to the system and the reasons it is not relevant
- DR5: The process for managing risk of the PKI operations in terms of both security and service integrity.

Section 4 – Audit Testing and Results

Summary

- Provides general introduction as to tests of controls and results
- Provides information as to types of testing conducted
- Details (by criteria) for all applicable WebTrust for CA and Baseline and Network Security Criteria

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests

- Have developed sample controls for baseline +NS (already in place for WebTrust for CA)
- This section’s template is about 180 pages long

Section 5 – Unaudited Management Comments

Summary

- Expected to detail managements plan to deal with outstanding BugZilla or other issues as well as exceptions found in detailed testing

Enhancement of CPA Canada Processes

CPA Canada is revamping processes with a goal to strengthen the program and add more rigor. Included in the changes are:

- Replacement of Webtrust.org with CPA Canada - https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/standards-other-than-cas/publications/overview-of-webtrust-services
    - Webtrust.org no longer supports current security protocols
    - New pages reside in CPA Canada secure website – newer, modern look and feel
    - Redirection of old webpages to corresponding new pages - mapping complete enabling all traffic to be directed to new webpages automatically
- New link will be www.cpacanada.ca/webtrust
- Can also go to CABF's website and follow the link to WebTrust information

Enhancement of CPA Canada Processes

More detailed application and process considerations for auditors, including international –

- Separation of practitioner enrollment application from trademark agreement sets stage for process automation

WebTrust for Certification Authorities – Practitioner Enrollment Application

WebTrust for Certification Authorities – Trademark Agreement

Enhancement of CPA Canada Processes

Seal management:

- New Seal Deployment document is under development
- Improved rigor on expired seals – new seal expiration document under development

Collaboration with Browsers:

- CPA Canada and browsers are working together to establish an automated process to feed seal and audit report IDs to browsers
- CPA Canada will notify browsers in the event a seal expires or is revoked.

CPA Canada

- **CPA Canada**

Gord Beal	Bryan Walker
Kaylynn Pippo	Taryn Abate
Janet Treasure	Annette DaRocha

- **Consultant to CPA Canada**

Don Sheehy (Vice –chair)

- **Task Force Members and Technical Support Volunteers**

Jeff Ward (chair)	BDO	Tim Crawford	BDO
Chris Czajczyc	Deloitte	Dan Adam	Deloitte
Donoghue Clarke	EY	Zain Shabbir	KPMG
David Roque	EY	Matt Jantzen	BDO
Eric Lin	EY	Adam Fiock	BDO

Reporting Structure/Roles

- Gord Beal – WebTrust falls into Guidance and Support activities of CPA Canada
- Janet Treasure – Seal system and licensing responsibility
- Bryan Walker –Licensing advisor
- Don Sheehy - Task Force and CABF liaison
- Jeff Ward - Chair of the WebTrust Task Force and primary contact
- All Task Force members provide WebTrust services to clients
- Volunteers are supported by additional technical associates and CPA Canada liaison but report to CPA Canada

Thank you.

Questions?