

# CA/Browser Forum Meeting

**WebTrust for CA Update**

**02/20/2020**

**Jeff Ward & Don Sheehy**

# Agenda

- “WETSI”
- Almost there !
- Current Status Of Updated WebTrust Documents
- Reporting Requirements and Sample Reports
- New Projects
- CPA Canada Update

# “WETSI” - CONTINUING DISCUSSIONS



# WETSI

- Recently shared framework for comments
- Continuing issues faced
- Potential for working together

# Almost there !

## 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
- In CPA Canada and AICPA – for editing

# Detailed Controls Reporting – March 2020

- **Field tested with some minor changes proposed to system description**
- **Final changes being made to US version**
- **Canadian and IFAC audit report being developed**
- **Expected release March/April 2020**
- **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)**
- **Will NOT be primary report for public seal**
- **Short form (current report) will be public facing report with seal**

# Detailed Controls Reporting – March 2020

- **Component report template 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 Information, such as Management comments

# 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
- Sample description has been prepared based on description criteria that were adopted from SOC 3 PKI and Cyber

# 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

# Current Status of Updated WebTrust Documents

## WebTrust for CA 2.2.1

- Effective for periods beginning on or after March 1, 2020
- Corrected typographical errors and general cleanup. No substantive change in content.

## WebTrust for Extended Validation vs 1.7.1

- Effective for periods beginning on or after March 1, 2020
- Updated EV SSL Audit Criteria to conform to EV SSL Guidelines v1.7.1 and other clarifications

# Current Status of Updated WebTrust Documents

## WebTrust Baseline + NS vs 2.5

- Effective for audit periods beginning on or after March 1, 2020.
- Updated SSL Baseline Audit Criteria to conform to SSL Baseline Requirements v1.6.7 and Network Security Requirements v1.3.
- Principle 2, Criterion 2.14 – clarified prohibition on underscore characters
- Principle 2, Criterion 4.1 – added the requirement to maintain the IP addresses validation method used
- Principle 2, Criterion 4.6 – Removed provision for certificates issued prior to 1 March 2018. Added additional restrictions on validation methods.
- Principle 2, Criterion 4.10 – Removed 2017 qualifier date for this criterion
- Principle 4, Criteria 3.5, 3.6 – conform to updates in Network Security Requirements v1.3 regarding the use of continuous automated system monitoring
- Principle 4, Criterion 3.7 – new criterion to require response to alerts generated by monitoring systems within 24 hours

# Current Status of Updated WebTrust Documents

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

**Next round of updates to take place in October 2020 (unless needed earlier)**

# Reporting Requirements and Sample Reports

- Search on [cpacanada/webtrust](https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria) 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>
  - Will be updated by CPA Canada shortly. Present view last 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

<i>Last Updated: 30-June-19</i>											
	RKGC <sup>7</sup>	Key Protection <sup>8</sup>	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 <sup>1</sup>	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 <sup>1</sup>	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 <sup>1</sup>	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 <sup>2</sup>	N/A	Required <sup>2</sup>	N/A	N/A	See footnote 3	See footnote 4	N/A	See footnote 9
Publicly-Trusted Government PKI - EV SSL	Required	Required	Required <sup>2</sup>	Required <sup>2</sup>	Required <sup>2</sup>	N/A	N/A	See footnote 3	See footnote 4	N/A	See footnote 9
Publicly-Trusted Government PKI - CS	Required	Required	Required <sup>2</sup>	N/A	Not Required	N/A	Required <sup>1,2</sup>	See footnote 3	See footnote 4	N/A	See footnote 9
Publicly-Trusted Government PKI - EV CS	Required	Required	Required <sup>2</sup>	N/A	Not Required	Required <sup>2</sup>	Required <sup>1,2</sup>	See footnote 3	See footnote 4	N/A	See footnote 9
Publicly-Trusted Government PKI - All other uses	Required	Required	Required <sup>2</sup>	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 <sup>5</sup>	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		1-Sep-17	1-Nov-17
WebTrust for CA	2.2		1-Jun-19	1-Jun-19
WebTrust for CA	2.2.1		1-Mar-20	1-Mar-20
WebTrust for CA - Extended Validation - SSL	1.6.2		1-Oct-17	1-Oct-17
WebTrust for CA - Extended Validation - SSL	1.6.8		1-Jun-19	1-Jun-19
WebTrust for CA - Extended Validation - SSL	1.7.1		1-Mar-20	1-Mar-20
WebTrust for CA - Extended Validation - Code Signing	1.4.1		1-Ocr-17	1-Oct-17
WebTrust for CA - SSL Baseline with Network Security	2.3		1-Feb-18	1-Feb-18
WebTrust for CA - SSL Baseline with Network Security	2.4		1-Jun-19	1-Jun-19
WebTrust for CA - SSL Baseline with Network Security	2.4.1		30-Jun-19	1-Jun-19
WebTrust for CA - SSL Baseline with Network Security	2.5		1-Mar-20	1-Mar-20
WebTrust for CA - Publicly Trusted Code Signing Certificates	1.0.1		1-Oct-17	1-Oct-17
WebTrust for RA	1.0		30-Apr-19	30-Apr-19

# New projects

- **Use of third party auditors in WebTrust engagements**
  - Subservice organizations
  - External RAs
- **Reporting changes –**
  - Service locations and other minor changes
  - Review of ongoing reports in view of standards updates

# 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](http://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?