CHARTERED PROFESSIONAL ACCOUNTANTS CANADA
COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

# CA/Browser Forum Meeting

## WebTrust for CA Update

## 10/22/2020

**Jeff Ward & Don Sheehy**

# Agenda

- “WETSI”
- Impact of COVID -19
- Practitioner Guidance
- Reporting Guidance
- Detailed Controls Reporting
- Current Status Of Updated WebTrust Documents
- Reporting Requirements and Sample Reports
- New Projects
- CPA Canada Update

# “WETSI”

# WETSI

- No direct discussions in past 4 months
- December virtual meeting in planning stage
- Continuing issues faced

# Impact of COVID-19

## Issued - Practitioner guidance for auditors on COVID-19

- Discussed areas that might impact auditors and CAs
- Potential for scope limitations in certain areas caused by inability to physically be onsite
- Provides examples of tools and approaches as best practices
- On CPA Canada's web site (https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services) www.webtrust.org will redirect you

## Issued - Practitioner guidance for reports on COVID-19

- Provides examples of potential audit reports
- Provided electronically to registered WebTrust practitioners

# Impact of COVID-19

## COVID- 19 Temporary WebTrust Seal

- Can be awarded in a limited circumstance
- All controls tested are ok, but scope limitation exists due to government mandated restrictions
- Good for 6 months – expectation that scope limitation will be eliminated at that point
- Seal is removed once scope once the “clean” opinion is issued, when it is determined a report will be qualified/modified, OR six months, whatever happens first
- Due to second wave – Task Force will assess whether changes are needed to process

# Practitioner guidance for auditors

## Practitioner guidance for auditors

- Task force handoff to CPA Canada in early 2020
- Delayed until 2021 - In editing
  - initially delayed due to COVID-19 projects
  - Now delayed due to AODA compliance - The Accessibility for Ontarians with Disabilities Act (**AODA**) is a law that sets out a process for developing and enforcing accessibility standards. Needs to be met for all materials on website effective January 1, 2021.
- Version combines US, Canada and International
- Provides examples of tools and approaches as best practices

# Reporting Guidance

## Updated Reporting Templates

- Updated for changes to standards etc. since 2017
- Reporting examples for US, Cdn. and International short-form reports
- Effective December 1, 2020
- Will be available on CPA Canada website once compliant with OADA

# Detailed Controls Reporting

- Field tested with some minor changes to system description
- Audit reports developed, US Canada and IFAC
- Still tweaking some limitation wording
- Will NOT be primary report for public seal
- Short form (current report) will be public facing report with seal

# Detailed Controls Reporting

- **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

# Current Status of Updated WebTrust Documents

## No changes since last meeting

- WebTrust for CA 2.2.1 (effective November 1 2020)
- WebTrust Baseline + NS vs 2.5 (effective November 1 2020)

## Changes

- WebTrust for Extended Validation vs 1.7.3 (effective November 1 2020) - Updated EV SSL Criteria to conform to EV SSL Guidelines v1.7.3 and other clarifications
- WebTrust for Publicly Trusted Code Signing vs 2.0 – updated for new CA/B requirements that combined both EV and Publicly trusted code-signing - effective???
- WebTrust for Extended Validation Code Signing vs 1.4.1 – deleted effective???

# Changes ( Cont’d)

- **WebTrust for RA 1.01**
  - Minor updates done to reflect changes in WebTrust since release 1.0
  - Reporting - Will have short-form and detailed reporting available
  - Effective November 1, 2020

Next round of updates to take place in 2021

# 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.

# New projects

- **Use of third party auditors in WebTrust engagements**
  - Subservice organizations
  - External RAs

# 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.

## Current Standing of Licensed Practitioners:

- CPA Canada's website lists all licensed practitioners
- Provides information on their status (good standing, revocation, suspension)
- Does not provide history of the practitioners' licensure

# CPA Canada

- **CPA Canada**

| | |
|---|---|
| Gord Beal | Bryan Walker |
| Kaylynn Pippo | Taryn Abate |
| Janet Treasure | Jennifer Griffiths |

- **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?