CA/Browser Forum Meeting

WebTrust for CA Update
June 21, 2017

Jeff Ward / Don Sheehy / Janet Treasure

CHARTERED PROFESSIONAL ACCOUNTANTS CANADA
COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Current Status

- WebTrust for CA 2.1
  - As you are aware, based on ISO 21188
  - WebTrust criteria based on frameworks publicly vetted that are generally available to the public
  - The Task Force does not create technical criteria
  - Have proposed changes for the CABF to consider, ballot, vet and vote

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Current Status

No updates for

- WebTrust EV
- WebTrust EV Code signing
- WebTrust Code signing
- WebTrust Baseline + NS

At present

- WebTrust for RA
  - Draft version needing CABF comments available soon
  - CABF input will clarify our path to completion – some of the critical issues are “how much security is needed”

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Updates to W4CA

- Updated introduction section,
- Removed references to WebTrust v1 for Business Practices Disclosures. All CP and CPS documents must now be structured in accordance with RFC 3647 (recommended) or RFC 2527.
- Updated the following criteria:
  - Criteria 1.1 and 1.2 – removed WebTrust v1 references
  - Criteria 2.1 and 2.2 – swapped order to be consistent with 1.1 and 1.2
  - Criterion 3.6 – Expanded scope to specifically address hypervisors and network devices

Updates to W4CA

- Criterion 3.7 – Expanded scope to specifically address system patching and change management activities
- Criterion 3.8 – Clarified scope to include requirement for backups of CA information and data to be taken at regular intervals in accordance with the CA's disclosed practices.
- **Criterion 4.5 – Clarified scope to include destruction of any copies of CA keys for any purpose, and added illustrative controls addressing formal key destruction ceremonies.**
- **Criterion 4.9 – New criterion added to address CA Key Transportation events**
- **Criterion 4.10 – New criterion added to address CA Key Migration events**
- Criterion 7.1 – Cross certificate requests added

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Audit reporting issues

- Consistency in reporting has been issue at times

- Types of audit opinions –
  - Unqualified/unmodified (clean)
  - Qualified (except for)
  - Adverse – the point where there are too many qualifications
  - Disclaimer – work is performed but the report states no opinion is being made by the auditor – these are rare

Audit reporting issues

- As part of reporting templates developed, will provide a sample report that discusses each section of the audit report to provide guidance to the browsers [what they should be looking for etc.]

- Will try to keep consistency in qualified reports – both US and Canada have options that will try to be limited

- Possible transmittal letter being addressed

- Distribution of qualified reports being considered for alternatives

Current Status

- Practitioner Audit Reports – US – have received AICPA comments to release updated reporting under SSAE 18. Some changes will be for modified reports.
- Canada and international reports undergoing minor updates to approved versions under CSAE 3000 and CSAE 3001. Task also includes Management Assertions that are given in qualified report scenarios.
- Practitioner guidance for auditors under development covering public and private CAs. Draft expected later this year.

Report Content Additions

Disclosure of Changes in Scope or Roots with no Activity

- During the year, various roots may be retired and may not be in use at the end of the reporting period. In addition, certain roots that are included in scope may not have issued any certificates. This information is important to users of the report and should be included.

Reporting When Certain Criteria Not Applicable as Services Not Performed by CA

- There will be situations where certain WebTrust criteria are not applicable as the CA does not perform the relevant CA service. (e.g. certificate rekey activities). In these scenarios, it is recommended that the auditor note in the audit report that the criteria were not audited.

Report Content Additions

List of Root and Subordinate CAs in Scope

- All reports issued must list all root and subordinate CAs that were subject to audit. For attestation engagements, this list should match the list provided in management's assertion.
- The names of the CAs should be presented in a manner consistent with how these names appear in applications that use the CA's certificate (for example, when viewing the certificate chain in a web browser). The most common method of identification would be the "Common Name (CN)" field in the "Subject" extension of each CA certificate.
- The list of CAs should be presented in a clear format. It is preferred to list the CAs in a referenced appendix.

Being discussed

- WebTrust for Delegated Third Party Providers (DTP)
  - Would include Cloud, OCSP, etc
  - Feedback from CABF on integration of WebTrust for RA
  - Basic guidance developed in past – issues will include extent of testing, report leverage, full SOC 2 vs specific testing

Criteria for integrity for Certificate Transparency databases

- Integrity now only face that 2 might have same content that could both be wrong
- Criteria and audit needed for public/user confidence and potential audit reliance

Some new and old issues

- Issues in Network Security still leading to qualifications – potential modification of the guidelines
- WebTrust for CA reports – should a more detailed version be created similar to SOC 2 (limited distribution/no seal). Cost and usefulness
- Cloud questions continuing to surface as well as DTP involvement, creating confusion and inconsistency on audit scope
- The audit standards have changed in US and Canada

CPA Canada – latest changes

- CPA Canada

Gord Beal	Janet Treasure
Kaylynn Pippo	Lori Anastacio
John Tabone	Bryan Walker

- Consultant to CPA Canada - Don Sheehy (Vice –chair)

- Task Force Members and Technical Support Volunteers

Jeff Ward (Chair)	BDO	Daniel Adam	Deloitte
Chris Czajczyc	Deloitte	Tim Crawford	BDO
Reema Anand	KPMG	Zain Shabbir	KPMG
David Roque	EY	Donoghue Clarke	EY

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Reporting Structure/Roles

- Gord Beal – WebTrust falls into Guidance and Support activities of CPA Canada
- Janet Treasure – Seal system responsibility / product responsibility
- Bryan Walker –Licensing advisor
- Don Sheehy - Task Force and CABF
- 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

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Thank you.

Questions??

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA