CHARTERED PROFESSIONAL ACCOUNTANTS CANADA
COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

CA/Browser Forum Meeting WebTrust for CA Update

Redmond June 7, 2023

Tim Crawford, Don Sheehy & Dave Chin

AGENDA

- Brief product update
- New projects
- Focus Redmond
    1. ISO 27099 impact
    2. Lifecycle event reporting
    3. Detailed Controls reporting
    4. S/MIME initial reporting
    5. Practitioner Guide

- CPA Canada Updates
    1. Practitioner Qualification
    2. New Seals
    3. Qualified Seals and Hosting
    4. Other Updates

WEBTRUST PRODUCT UPDATE

NOW POSTED TO CPA CANADA SITE

What is New

- Network Security V1.0
  - CAB offerings (Baseline, Codesigning and S/MIME) incorporate the NS requirements by reference
- WebTrust for S/MIME V1.0
- WebTrust - Short Form Reports - Registration Authorities
- WebTrust - Illustrative Examples - Force Majeure Event Scope Limitation Practitioner Reports

NOW POSTED TO CPA CANADA SITE

Updates

- WebTrust for Baseline with Network Security V2.7.
- WebTrust for Code Signing V3.2
- WebTrust for EV V1.8
- WebTrust for VMC V1.4
- See https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

NOW POSTED TO CPA CANADA SITE

Updates

- WebTrust - Canada reporting under CSAE 3000 - 3001
- WebTrust - U.S. reporting under SSAE 18
- WebTrust - International reporting under ISAE 3000
- WebTrust for Certification Authorities - Engagement Applicability Matrix (April 1st, 2023)

IN PROCESS

Now Being Updated

- **WebTrust for CA 2.2.2**
  - Impact ISO 27099 being assessed
  - Some front-end discussion needs to be reworked
- **WebTrust for RA 1.1**
  - Some front-end discussion needs to be reworked
  - Impact of ISO 27099 changes to W4CA
  - Review changes to relevant CA/B docs that are used

NEW PROJECTS

WebTrust for CA Supporting X9

- X9 is a standard setting organization for financial institutions and supporting organizations
- X9 has identified a long list of PKI use cases in the financial sector
- A base CP has been developed and creating a business plan to use WebTrust in the compliance requirements

WebTrust Supporting IoT Programs

- A number of smaller IoT programs require a WebTrust engagement for admission
- Evaluating other programs and the use of external service providers

1. IMPACT OF ISO 27099 ON W4CA

Information technology — Public key infrastructure — Practices and policy framework - First edition 2022/07

PRELIMINARY REVIEW

- In this current ISO version – we now have over 400 ‘shall’ vs. the ‘should’ that were in pre-2018 version
- Other changes that will need to address
  - New criteria
  - Changes in controls (both additions, deletion and wording changes)
  - Criteria deleted
  - Criteria changed into controls and prior controls deleted

PRELIMINARY REVIEW

- To implement an ISO International Standard and other normative ISO deliverables …"shall" indicates a requirement. "should" indicates a recommendation. "may" is used to indicate that something is permitted.
- Issues
  1. Should all of these over 400 controls be mandatory controls vs illustrative with potential of using mitigating or compensatory controls?
  2. Impact on WebTrust engagements

ISO 27099

New Criteria – for example

- Subscriber and relying party agreements
- Controlled CA Termination
- Root CA controls – covering a number of areas
- CA Key Generation - for device testing, restricted access to hardware and functioning

ISO 27099

New Controls – for example

- Subscriber and relying party agreements – breakdown of controls for subscriber agreement, relying party agreement, multiple component services, subject key compromise
- Application access control - Include optional controls specified in ISO/IEC 27002:2022, Clause 5 for guidance on object reuse.
- Business continuity - 3 new controls introduced
- Key generation – 6 new controls introduced
- CA key destruction – 5 new controls introduced

ISO 27099

Deleted Controls – for example

- CA certificate life cycle management controls– subordinate CA certificate – deleted all 13 controls and replaced by prior 6 control objectives as controls
- Certificate Revocation – deleted 3 controls
- Certificate Renewal - deleted 6 controls
- Audit log protection and retention – deleted 3 controls

IMPACT OF CHANGE

- What were illustrative controls before may now become mandatory
- Not meeting mandatory controls – qualified reports?
- Not allowing for compensating controls?
- New Criteria and controls to deal with

2. LIFECYCLE REPORTING

- As all are aware separate reports exist for certain lifecycle events when they occur during the period.
  - Root key 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)
  - Key Transportation
  - Key Migration
  - Key Destruction (Death Certificate)

LIFECYCLE REPORTING

- **Current issue being addressed by TF "What happens if one of these events do not occur during the period?"**
  - Option 1
    - As presently done – no disclosure
    - Option for separate reports to be submitted that covers the event (esp Key Gens)
  - Option 2
    - Disclose fact the event did not occur in separate paragraph so could not be tested
      - Pro
        - Provides additional information on events and criteria not covered in current audit
        - Currently done for explicit **services** not performed (for example escrow)
        - Consistency with SOC 2 detailed reports
      - Cons
        - Sections are listed as "if applicable" so if no event, why disclose and lead to even longer audit reports?
        - Will lead to potential misunderstanding of audit report
  - TF is looking at both options with no decision yet

3. DETAILED CONTROLS REPORTING

- Current version has been modified for changes in BR and NS relevant criteria
- Need to finalize WTCA before new version release
- Minor report changes in audit report and system description
- Will NOT be primary report for public seal
- Short form (current report) will be public facing report with seal

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

DETAILED CONTROLS REPORTING

Section 1 – Independent Practitioners Report

- Based on SOC 2 and WebTrust
- Template is about 3 pages
- Sets out
  - Scope
  - CA Responsibilities for controls
  - Service Auditor Responsibilities
  - Inherent Limitations
  - References tests of controls
  - Opinion
  - Restricted Use

DETAILED CONTROLS REPORTING

Section 2 – Managements Assertion

- Based on SOC 2 and WebTrust templates
- Template is about 1 1/2 pages
- Sets out
  - Scope
  - CA Responsibilities for controls
  - Assertion

DETAILED CONTROLS REPORTING

Section 3- Description criteria and system description

- Based on SOC 2, CA/B asks and WebTrust
- Template is about 22 pages but with appropriate detail may double
- Sets out
  - Scope & Boundaries for System
  - Detailed Audit Coverage
    - Services Provided and not provided
    - Scope of description
    - System incidents
  - Components of System
    - Infrastructure
    - Software
    - People
    - Procedures
    - Data

DETAILED CONTROLS REPORTING

Section 3- Description criteria and system description

- Description of Controls Relevant to WebTrust Principles
  - CA Business Practice Disclosure
  - CA Business Practices Management
  - CA Environmental Controls
    - Security Mgt
    - Risk Assessment
    - Vendor (Third Party)
    - Personnel Security
    - Physical and environmental security (including Locations)
      - Operations Mgt
      - System access mgt
      - Network Security
      - Physical Access and Secure Zone
  - Systems Development, Change Mgt and Maintenance

DETAILED CONTROLS REPORTING

Section 3- Description criteria and system description

- Description of Controls Relevant to WebTrust Principles
    - Covers controls relevant to all principles including for example
        - Disaster recovery backup and business continuity mgt
        - Monitoring and compliance
        - CA Key generation
        - CA Key Storage, Backup, and Recovery
        - CA Key Public Distribution
        - CA Key Usage
        - CA Key Archival
        - CA Key Destruction
        - CA Key Compromise
        - CA Cryptographic Hardware Life Cycle Management
        - CA Key Transportation
        - CA Key Migration (if applicable)

DETAILED CONTROLS REPORTING

Section 3- Description criteria and system description

- Description of Controls Relevant to WebTrust Principles
    - CA-Provided Subscriber Key Generation Services
    - Integrated Circuit Card (ICC) Lifecycle Management
    - Requirements for Subscriber Key Management
    - Subscriber Registration
    - Certificate Renewal
    - Certificate Rekey
    - Certificate Issuance
    - Certificate Distribution
    - Certificate Revocation
    - Certificate Validation
    - Subordinate CA Certificate and Cross Certificate Lifecycle Management

DETAILED CONTROLS REPORTING

Section 4- Detailed testing performed and results thereof

Sets out controls by criteria, tests performed and results

Criteria	Controls	Tests of Controls performed	Results of tests

Template is 211 pages for this section using W4CA, BR and NS

DETAILED CONTROLS REPORTING

Section 4- Detailed testing performed and results thereof – some examples

Criteria	Controls	Tests of Controls performed	Results of tests
Personnel security			
The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	3.3.11 - Physical and logical access to CA facilities and systems is disabled upon termination of employment.	Obtained list of employees terminated during the year For a sample of terminated employees: • Reviewed relevant documentation showing that physical access card was returned upon termination • Reviewed access logs for evidence that logical access was removed within 24 hours	No exceptions noted

DETAILED CONTROLS REPORTING

Section 4- Detailed testing performed and results thereof –scenarios for same control

Criteria	Controls	Tests of Controls performed	Results of tests
Personnel security			
The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	**3**.3.11 - Physical and logical access to CA facilities and systems is disabled upon termination of employment.	Obtained list of employees terminated during the year For a sample of terminated employees: • Reviewed relevant documentation showing that physical access card was returned upon termination • Reviewed access logs for evidence that logical access was removed within 24 hours	Exception Noted For 1 of 10 employees tested, logical access rights were not revoked for 3 weeks.

DETAILED CONTROLS REPORTING

Section 4- Detailed testing performed and results thereof –scenarios for same control

Criteria	Controls	Tests of Controls performed	Results of tests
Personnel security			
The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	3.3.11 - Physical and logical access to CA facilities and systems is disabled upon termination of employment.	The circumstances that warrant the operation of this control did not occur during the examination period, this control could not be tested. To obtain evidence that there were no terminations compared employee list at end of prior year to list at current year.	Since the circumstances that warrant the operation of this control did not occur during the examination period, this control could not be tested.

DETAILED CONTROLS REPORTING

Section 4- Detailed testing performed and results thereof

- Just looked at three common scenarios
- Impact on audit report?
- What happens when control becomes mandatory?
    - Appropriate and timely actions shall be taken when employment is terminated so that controls (e.g. access controls) are not impaired.

DETAILED CONTROLS REPORTING

Section 5- Other Information that is not covered by auditors report

This section will discuss issues that were identified in the audit (or reported to Bugzilla) for which management wants to discuss the remediation that has been undertaken or is planned to be undertaken.

DETAILED CONTROLS REPORTING

Section 6- List of CAs in scope

This section will set out CAs in scope, revoked, etc. during year

4. S/MIME

WebTrust criteria and reporting are available on CPA Canada website

- Only issue – reporting periods
- Need agreement by Browsers as to when to report on S/MIME
- Also use of Point in Time vs Period of Time

5. PRACTITIONER GUIDANCE

Current modifications

- Updated to reflect standards changes to March 2023
- Updated and added section on what is PKI and background
- Added Force Majeure scenario in appendix
- Added Auditor qualifications letter to Mozilla
- Updating based on SOC 2 US guide changes
- Browser and delegated WebTrust member to work together to June to fully develop use of software and IT audit techniques on available Certificate database information
- TF members are reviewing – any detailed comments by end of June

CPA CANADA WEBTRUST UPDATE

1. Practitioner Qualification
2. New Seals
3. Qualified Seals and Hosting
4. Other

MEET THE WEBTRUST AUDIT TEAM

Qualifications

Audit Firm

Professional accounting and auditing firm

1. Member in good standing with the National Accounting Organization that is a member of International Federation of Accountants (IFAC)
2. Licensed to provide assurance services in the countries where it provides WTCA
3. Demonstrate an understanding of systems related to the issuance of digital certificates
4. Experience in Certificate Authority assessment and Public Key Infrastructure
5. Professional Liability insurance minimum $1 million USD

Signing Partner
QA Partner

Practitioner Qualifications

Same as 1, 2, 3 & 4

Field Staff

1. Maintain IT specialist certification (e.g., CISA, CISM, etc.)
2. Be familiar with the requirements established by the CA/Browser Forum and the WebTrust Principles and Criteria associated with the assessment being performed.

WEBTRUST NEW SEALS FOR 2023

Hosting Infrastructure ready for all new seals

S/MIME effective September 1, 2023

Network Security effective July 1, 2023

Registration Authorities available March 1, 2023

Qualified Report Mark for all individual seals available March 1, 2023

WEBTRUST SEALS QUALIFIED

Qualified Report - “Audit Reports that are fairly stated except for …….”

- **CPA Canada is now hosting qualified reports**
- **A qualified report Mark is available for all Seals**

CPA CANADA UPDATES

WebTrust Pricing Strategy

- CPA Canada completed Practitioner Licensing pricing review.
  - New Practitioner Licensing increase effective July 1, 2023
- Seal pricing strategy is currently under review with completion planned for September 2023

New for F2024 (Currently under development)

- Practitioner Secure login in the works
- Practitioner guide
- Training programs

WEBTRUST KEY PLAYERS

- CPA Canada

  Anna–Marie Christian
  Dave Chin **(Co-Chair)**
  Lilia Dubko
  Reza Harji

- Consultant to CPA Canada

  Don Sheehy

- Task Force Members

  Tim Crawford **BDO (Co-Chair)**
  Eric Lin **EY**
  Donoghue Clarke **EY**
  Zain Shabbir **KPMG**
  Chris Czajczyc **Deloitte**
  Dan Adam
  Adam Fiock **BDO**

THANK YOU

QUESTIONS?