



# CA/Browser Forum Meeting WebTrust for CA Update

Tim Crawford, Don Sheehy, Anna-Marie Christian and Dave Chin

October 2023

# Agenda



- Brief Product Update
- Focus Portsmouth
  1. Practitioner Guide
  2. Detailed Controls Reporting
  3. Impact of ISO 27099 On W4CA
  4. Lifecycle Event Reporting
  5. New Reporting Recommendations
  6. Other Projects Task Force is Working On
- CPA Canada Updates
  1. New WebTrust Task Force Members
  2. Signing Practitioner vs Quality Assurance Practitioner
  3. New Seal Pricing and Bundles
  4. Seal Updates



# New Posted to CPA Canada Site

- WebTrust for S/MIME V1.0.1
- WebTrust – Combined US/International report (coming)



# New Posted to CPA Canada Website

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



# New Posted to CPA Canada Website

## 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>



# In Progress

## Updates in progress

### WebTrust for CA 2.2.2

- Impact ISO 27099 was 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



# In Progress

## Updates in progress

### Reporting Templates

- Inclusive examples
- Qualified seal updates
- Updated Canadian and International reports for transitional issues
- Updating reports when issuing Network Security separately



# 1. Practitioner Guidance

Finalized

- Updated to reflect standards changes to March 2023
- Updated and added section on what is PKI and background
- Updating based on SOC 2 US guide changes
- Browser and delegated WebTrust members added additional material on software and IT based interrogation audit techniques for available Certificate database information
- Added Force Majeure scenario in appendix
- Added Auditor qualifications letter to browsers as appendix
- Over 175 pages in current form
- Approved for publication by Task Force Sept 19





# 2. Detailed Controls Reporting

- Current version has been updated for changes in BR and NS relevant criteria
- Report changes and system description modifications
- Added additional illustrative assertion and additional paragraph to audit report for service organizations
- Will NOT be primary report for public seal
- Illustrative template is now 218 pages ( Wt4CA, BR and NS)
- Short form (current report) will be public facing report with seal
- Approved for publication by Task Force Sept 19



# 2. Detailed Controls Reporting

**Component report template has been developed based on period of time report– (PIT 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 6 – List of CAs in scope



# 2. Detailed Controls Reporting

Audit report – reflecting inclusive approach



*(Insert as a third paragraph when inclusive method of reporting is used for service organizations)*

ABC-CA uses QRS Data Storage, Inc. [name of service organization] (service organization) to provide data centre services [describe services provided by service organization]. ABC-CA s description includes a description of QRS Data Storage, Inc. services used by ABC-CA, including the controls of QRS Data Storage, Inc. and the controls designed by ABC-CA and operated by QRS Data Storage, Inc. that are necessary, in combination with controls at ABC-CA, for ABC-CA to achieve the applicable WebTrust Criteria.



# 3. Impact of ISO 27099 On W4CA



## Information technology

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

# 3. ISO Preliminary Assessment



- In this current ISO version – we now have over 400 ‘shall’ vs. the ‘should’ that were in pre-2018 21188 version
- Other changes to be addressed
  - New criteria
  - Changes in controls (both additions, deletion and wording changes)
  - Criteria deleted
  - Criteria changed into controls and prior controls deleted
  - References to other ISO docs

# 3. ISO Preliminary Assessment



- Prepared rough draft of WebTrust 3.0 using 27099
- Too many issues such as general references to inclusion of ISO 27002
- Have reached out for clarification on 27002 content
- At this point will continue to assess but unlikely to see anything before 2025
- Will continue to assess whether any changes are needed to WT4CA 2.2.2 in meantime



# 4. 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)



# 5. New Reporting Issues



- Management assertion by service provider
- Additional reporting paragraph to acknowledge service provider





# 5. New Reporting Issues



- Effective April 1<sup>st</sup>, 2024, recommend practitioners to issue a separate Network Security report to support updated audit principles and criteria.



# 6. Other Projects Task Force is Working On



## 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



# WebTrust Update



## CPA Canada Updates

- New WebTrust Task Force Members
- Signing Practitioner vs Quality Assurance Practitioner
- New Seal Pricing and Bundle
- Seal Updates



# New WebTrust Task Force Members

## **Jinhwan Shin from Deloitte Korea** – First International WT Task Force Member

- serves as a Director at Deloitte Anjin LLC, also known as Deloitte Korea
- actively participates in international projects focused on National PKI development, collaborating with national Root CAs and governmental organizations in various Asian and African countries
- contributed to International Development Business for the establishment of National PKI and ODA (Official Development Assistance) for PKI consulting projects
- experienced feasibility study and implementation projects for National PKI establishment in Panama, Costa Rica, Cameroon, Kenya, Mongolia, Iran, the Philippines, and Indonesia

## **David Lachmansingh from Richter Canada**

- Partner at his firm
- WebTrust practitioner from Toronto
- over 18 years of experience delivering audit and security expertise in the areas of IT risk management to many industry sectors.



# Signing Practitioner vs Quality Assurance Practitioner

## Signing Practitioner

1. Member in good standing with their National Accounting Organization that is a member of International Federation of Accountants (IFAC) – global organization of the accounting profession
2. Licensed to provide assurance services in the countries where it provides WTCA
3. Demonstrates an understanding of systems related to the issuance of digital certificates
4. Experience in Certificate Authority assessment And Public Key Infrastructure

## Quality Assurance Practitioner

- Includes both 3. and 4.
- 1. and 2. recommended but not mandatory
- QA employee may not necessarily be an audit partner



# New WebTrust Seal Hosting Fees Effective January 1, 2024



**WebTrust for CA -  
\$4K, previously \$3K**



**Standalone SSL  
Baseline without  
Network Security \$3K**



**Standalone Network  
Security \$3K**

**CPA Canada will offer bundled pricing for WTCA + BR-SSL + NS at \$8K**



# Seal Updates

## Registration Authorities

- First RA seal for PSW Group GmbH issued September 2023

## S/MIME

- Seal infrastructure in place as of September 1, 2023

## Qualified Seal

- Launched July 1, 2023
- Recommendation included in CCADB: “Qualified opinion should have a WebTrust Seal”



Registration Authorities



S/MIME



Qualified Seal



# Enrolled WebTrust Practitioners: International



## Practitioners

- Anthony Kam & Associates Ltd.
- AUDIT CPA
- AUDIT TRUST SERVICES S.A.S.
- AUREN
- Baker Tilly MH Consulting Sdn Bhd
- BDO
- Crowe FST Audit Ltd
- Deloitte
- Digital Age Strategies Pvt Ltd. – NEW Example
- EY
- KPMG
- Kochar Consultants P. Ltd (India) “**New**”
- Moreira Associados Auditores Independentes
- PKI Contabilidade e Auditoria Ltda
- PwC
- Richter LLP
- RSM Hong Kong
- Schellman & Company, LLC
- Sun Rise CPAS’ Firm, Member Of DFK International





# Task Force Members



## **CPA Canada**

Anna-Marie Christian  
Dave Chin (Co-Chair)

Lilia Dubko  
Reza Harji

## **Consultant to CPA Canada**

Don Sheehy (Former Co-Chair)

## **Task Force Members**

Tim Crawford, BDO (Co-Chair)  
Chris Czajczyc, Deloitte  
Donoghue Clarke, EY  
Eric Lin, EY  
Adam Fiock, BDO

Zain Shabbir, KPMG  
Dan Adam  
David Lachmansingh, Richter LLP  
Jinhwan Shin, Deloitte



Thank you!  
Questions?

