CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

CA/Browser Forum Meeting

WebTrust for CA Update

June 13, 2019

Jeff Ward & Don Sheehy

Agenda

- “WETSI”
- Current Status Of Updated WebTrust Documents
- Reporting Requirements and Sample Reports
- Current Status Of Other WebTrust Task Force Projects
- New “Lifecycle” Reports
- SOC 2 Like Reporting
- Reporting Terminology
- Brief CPA Canada Update

“WETSI” - CONTINUING DISCUSSIONS

CHARTERED PROFESSIONAL ACCOUNTANTS CANADA
COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Following Berlin

- WebTrust Seal vs ETSI certification understanding
- Terminology – moving to common language
- Continuing issues faced
- Potential for working together

Current Status of Updated WebTrust Documents

WebTrust Baseline + NS vs 2.4

- Effective for periods beginning on or after June 1, 2019
- Updated SSL Baseline Audit Criteria to conform to SSL Baseline Requirements v1.6.2 and Network and Certificate System Security Requirements v1.2
- Principle 1, Criterion 5 – The CA's CP and CPS must now follow RFC 3647 format. RFC 2527 has been sunset.
- Principle 2, Criterion 2.14 – new criterion added to address certificates with underscore characters. Criteria 2.14-2.16 renumbered to 2.15-2.17.
- Principle 2, Criterion 4.6 – Re-validations cannot use methods 3.2.2.4.1 and 3.2.2.4.5 as of 1 August 2018
- Principle 2, Criteria 5.2, 5.3 and 5.4 – Updated revocation criteria and timelines
- Principle 4 – Updates made to conform to CA/B Forum Ballot SC3

Current Status of Updated WebTrust Documents

WebTrust for CA 2.2

- Effective for periods beginning on or after June 1, 2019
- Minor updates made to conform to ISO 21188:2018 Edition

WebTrust for Extended Validation vs 1.6.8

- Effective for periods beginning on or after June 1, 2019
- Principle 1, Criteria 4 – RFC 3647 requirement with the sunsetting of 2527
- Principle 2, Criteria 5.2-5.4 – updated revocation requirements based on changes to BRs

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

Current Status of Updated WebTrust Documents

WebTrust for RA vs 1.0

- Effective for periods beginning on or after April 30, 2019
- Provides a framework for third party assurance providers to assess the adequacy and effectiveness of the controls employed by a Registration Authority (RA) that performs either a portion or all of the registration related functions for a Certification Authority (CA) on an outsourced basis.
- Audit guidance for registration functions that are conducted directly by the CAs entirely are covered in the document, WebTrustSM/TM Principles and Criteria for Certification Authorities.

Reporting Requirements and Sample Reports

- 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

- Sample reports have been developed under each standard since W4CA program began – current ones are at https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/practitioner-qualification-and-guidance

WebTrust Reports Available – Full Lifecycle

- Rootkey Generation Ceremony Report (Birth Certificate)
- New - 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 they are operating effectively)
- New - Key Transportation, Migration & Destruction (under development)

Other WebTrust Program Components

WebTrust Audit Applicability

Based on current CA/Browser Forum and Other Requirements

Last Updated: 1-May-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

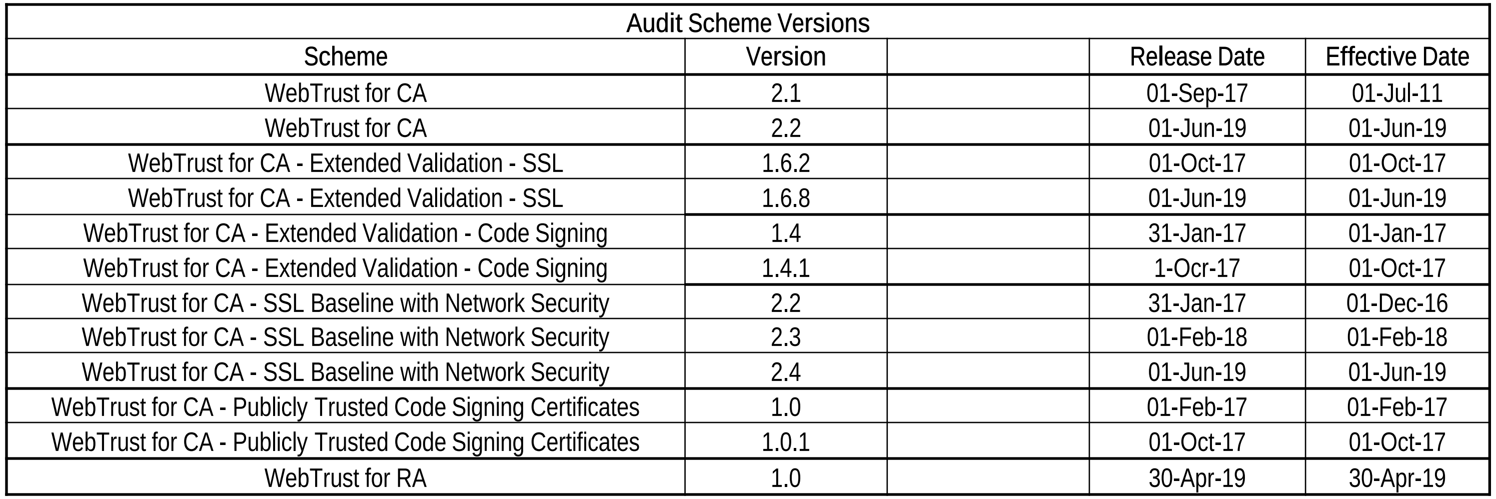
[7] RKGC refers to audit reports to be issued in conjunction with a WebTrust Auditor's witnessing of CA's Root Key Generation Ceremony.

[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.

CHARTERED PROFESSIONAL ACCOUNTANTS CANADA
COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Other WebTrust Program Components



Audit Scheme Versions				
Scheme	Version		Release Date	Effective Date
WebTrust for CA	2.1		01-Sep-17	01-Jul-11
WebTrust for CA	2.2		01-Jun-19	01-Jun-19
WebTrust for CA - Extended Validation - SSL	1.6.2		01-Oct-17	01-Oct-17
WebTrust for CA - Extended Validation - SSL	1.6.8		01-Jun-19	01-Jun-19
WebTrust for CA - Extended Validation - Code Signing	1.4		31-Jan-17	01-Jan-17
WebTrust for CA - Extended Validation - Code Signing	1.4.1		1-Ocr-17	01-Oct-17
WebTrust for CA - SSL Baseline with Network Security	2.2		31-Jan-17	01-Dec-16
WebTrust for CA - SSL Baseline with Network Security	2.3		01-Feb-18	01-Feb-18
WebTrust for CA - SSL Baseline with Network Security	2.4		01-Jun-19	01-Jun-19
WebTrust for CA - Publicly Trusted Code Signing Certificates	1.0		01-Feb-17	01-Feb-17
WebTrust for CA - Publicly Trusted Code Signing Certificates	1.0.1		01-Oct-17	01-Oct-17
WebTrust for RA	1.0		30-Apr-19	30-Apr-19

Current Status of Other WTF Projects

Practitioner guidance for auditors

- Under development covering public and private CAs
- Version for US, Canada and International
- Will provide examples of tools and approaches as best practices
- Latest draft reviewed May 2019 meeting – expected release by end of 2019

SOC 2 Like Reporting

- **Shell 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 Management comments
- **In essence, asking for reports that have detail similar to an AICPA SOC 2 report (SOC 2 reports issued on restricted distribution basis by audit profession for service organizations)**
- **Expected completion late 2019**

Section 1 – Audit report

Summary

- Draft 1 - About 5 pages long for US version
- Reporting on 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
- Sets out restricted use

Section 2 – Management Assertion

Summary

- Developed using WebTrust for CA and SOC 2
- Required for all engagements

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
- Draft 1 at present based on comparison of RFC 3647, SOC 2 and SOC cyber

Description Criteria

- DC1: The nature of the entity’s business and operations, including the principal products or services the entity sells or provides and the methods by which they are distributed
- DC 2: The principal service commitments and system requirements. This will include uptime commitments for business resumption, principal types of sensitive information created, collected, transmitted, used, or stored by the entity and others deemed important by the entity or significant third party users.
- DC 3: The components of the system to provide the services, including the following:
  a. Infrastructure b. Software c. People d. Procedures e. Data

Description Criteria

- DC 4: For identified system incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements, as of the date of the description (for a type 1) or during the period of time covered by the description (for a type 2), as applicable, the following information

    a. Nature of each incident

    b. Timing surrounding the incident

    c. Extent (or effect) of the incident and its disposition

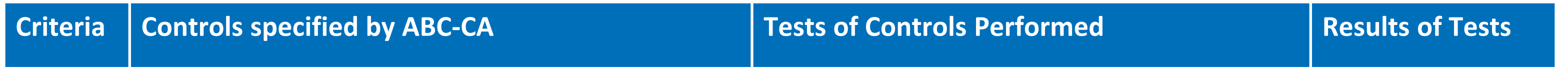
Description Criteria

- DC 5: Any specific applicable trust services criterion that is not relevant to the system and the reasons it is not relevant
- DC6: The process for managing risk of the PKI operations in terms of both security and service integrity.

Section 4 – Audit Testing and Results

Summary

- Provides general intro 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

- We are developing 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 WTF Projects – Lifecycle Reports

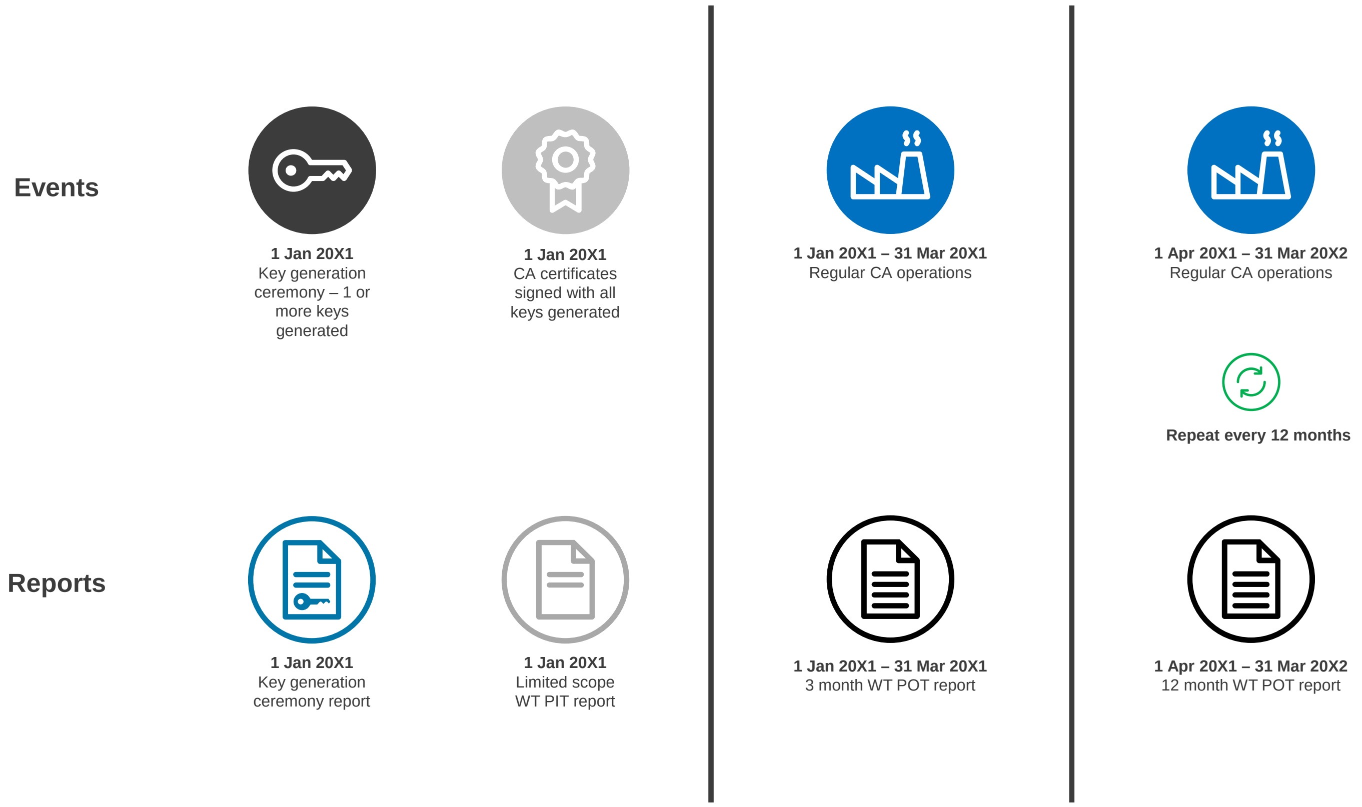
- Regular reports – based on various event scenarios
- Event reports for key generation, key protection, transport, migration and destruction to cover all expected events cradle to grave

Types of Reports

- WebTrust for CA Report (includes CA, EV SSL, EV Code Sign, and Baseline Requirements reports as applicable to the CA's use case)
- Limited Scope WebTrust for CA Report (does not include controls surrounding Subscriber Key Generation services and End-Entity Certificate Lifecycle Management Activities as these have not yet occurred)
- Key Generation Ceremony Report
- Key Lifecycle Protection Report (includes CA Key Lifecycle Management and Physical and Environmental Security controls.

PIT = Point-in-time report (i.e. as at a singular date)
POT = Period-of-time report (i.e. covering a period of dates)

Scenario 1: New CA, key generation and immediate start to operations



Events

1 Jan 20X1
Key generation ceremony – 1 or more keys generated

1 Jan 20X1
CA certificates signed with all keys generated

1 Jan 20X1 – 31 Mar 20X1
Regular CA operations

1 Apr 20X1 – 31 Mar 20X2
Regular CA operations

Repeat every 12 months

Reports

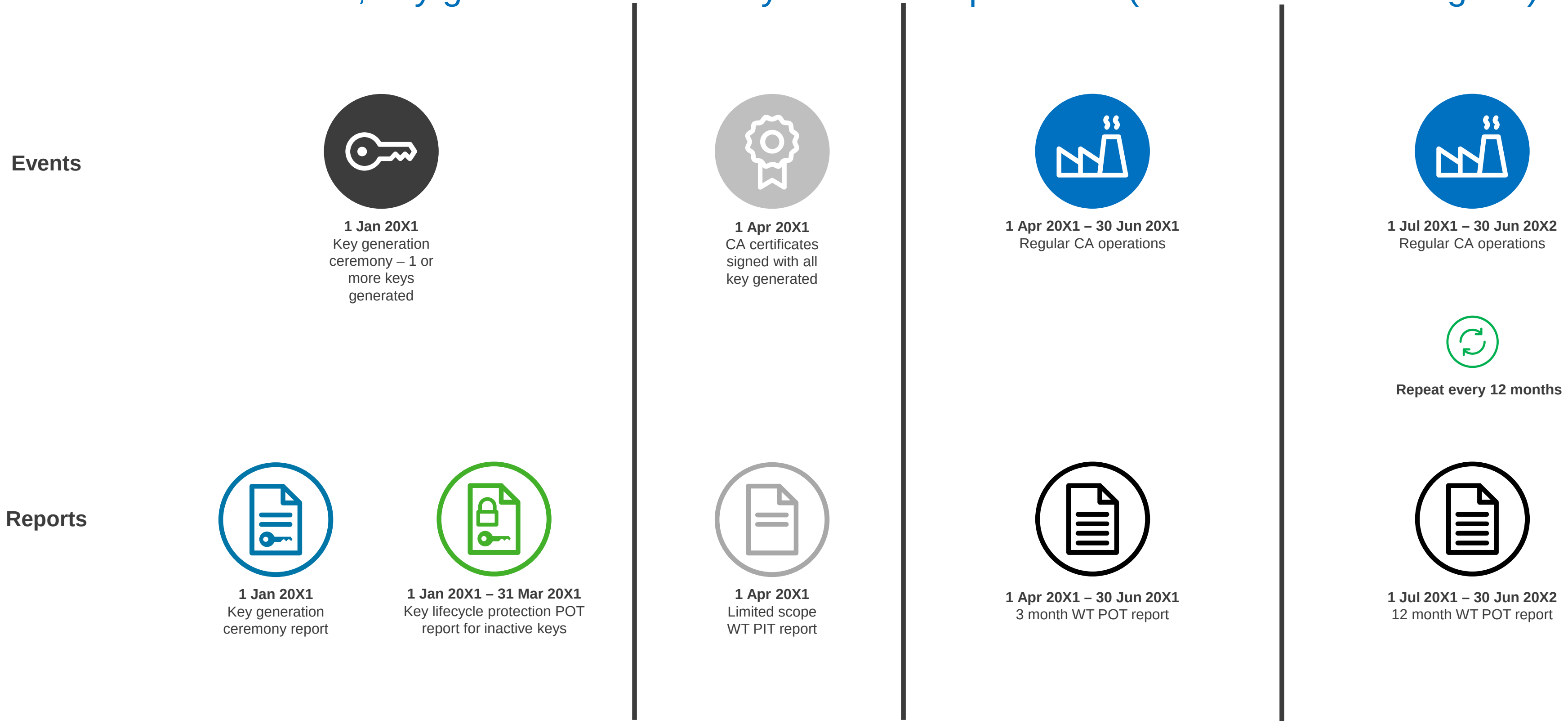
1 Jan 20X1
Key generation ceremony report

1 Jan 20X1
Limited scope WT PIT report

1 Jan 20X1 – 31 Mar 20X1
3 month WT POT report

1 Apr 20X1 – 31 Mar 20X2
12 month WT POT report

Scenario 2: New CA, key generation and delayed start to operations (CA certificate not signed)

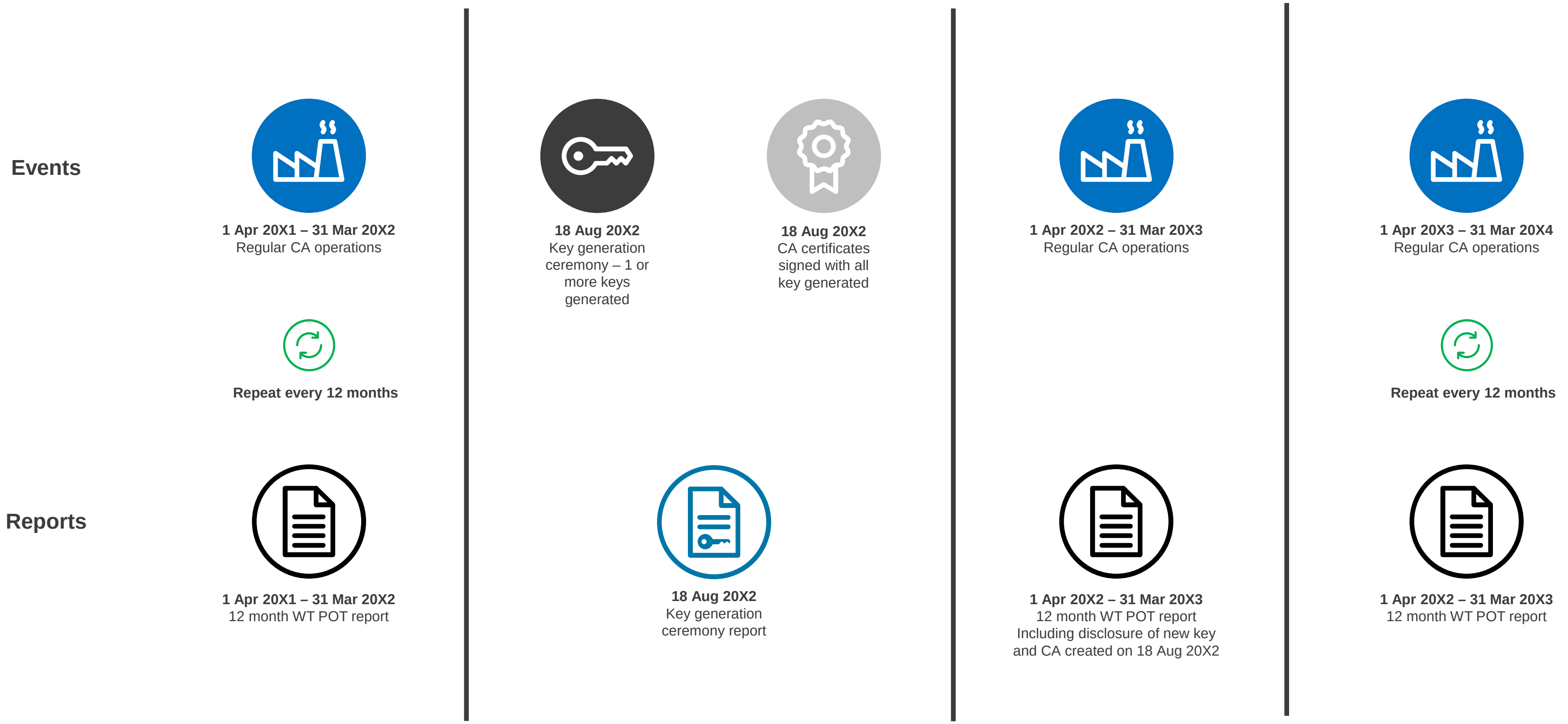


Events	**1 Jan 20X1** Key generation ceremony – 1 or more keys generated	**1 Apr 20X1** CA certificates signed with all key generated	**1 Apr 20X1 – 30 Jun 20X1** Regular CA operations	**1 Jul 20X1 – 30 Jun 20X2** Regular CA operations **Repeat every 12 months**
Reports	**1 Jan 20X1** Key generation ceremony report **1 Jan 20X1 – 31 Mar 20X1** Key lifecycle protection POT report for inactive keys	**1 Apr 20X1** Limited scope WT PIT report	**1 Apr 20X1 – 30 Jun 20X1** 3 month WT POT report	**1 Jul 20X1 – 30 Jun 20X2** 12 month WT POT report

Scenario 3: New CA, key generation and immediate start to operations with some parked keys for future use

Events	**1 Jan 20X1** Key generation ceremony – multiple	**1 Jan 20X1** CA certificates signed with some key generated	**1 Jan 20X1 – 31 Mar 20X1** Regular CA operations		**1 Apr 20X1 – 31 Mar 20X2** Regular CA operations **Repeat every 12 months**	
Reports	**1 Jan 20X1** Key generation ceremony report	**1 Jan 20X1** Limited scope WT PIT report	**1 Jan 20X1 – 31 Mar 20X1** 3 month WT POT report	**1 Jan 20X1 – 31 Mar 20X1** Key lifecycle protection POT report for all inactive keys	**1 Apr 20X1 – 31 Mar 20X2** 12 month WT POT report	**1 Apr 20X1 – 31 Mar 20X2** Key lifecycle protection POT report for all inactive keys

Scenario 4: Existing CA, additional key generation for new CA during the period



Events

1 Apr 20X1 – 31 Mar 20X2
Regular CA operations

Repeat every 12 months

18 Aug 20X2
Key generation ceremony – 1 or more keys generated

18 Aug 20X2
CA certificates signed with all key generated

1 Apr 20X2 – 31 Mar 20X3
Regular CA operations

1 Apr 20X3 – 31 Mar 20X4
Regular CA operations

Repeat every 12 months

Reports

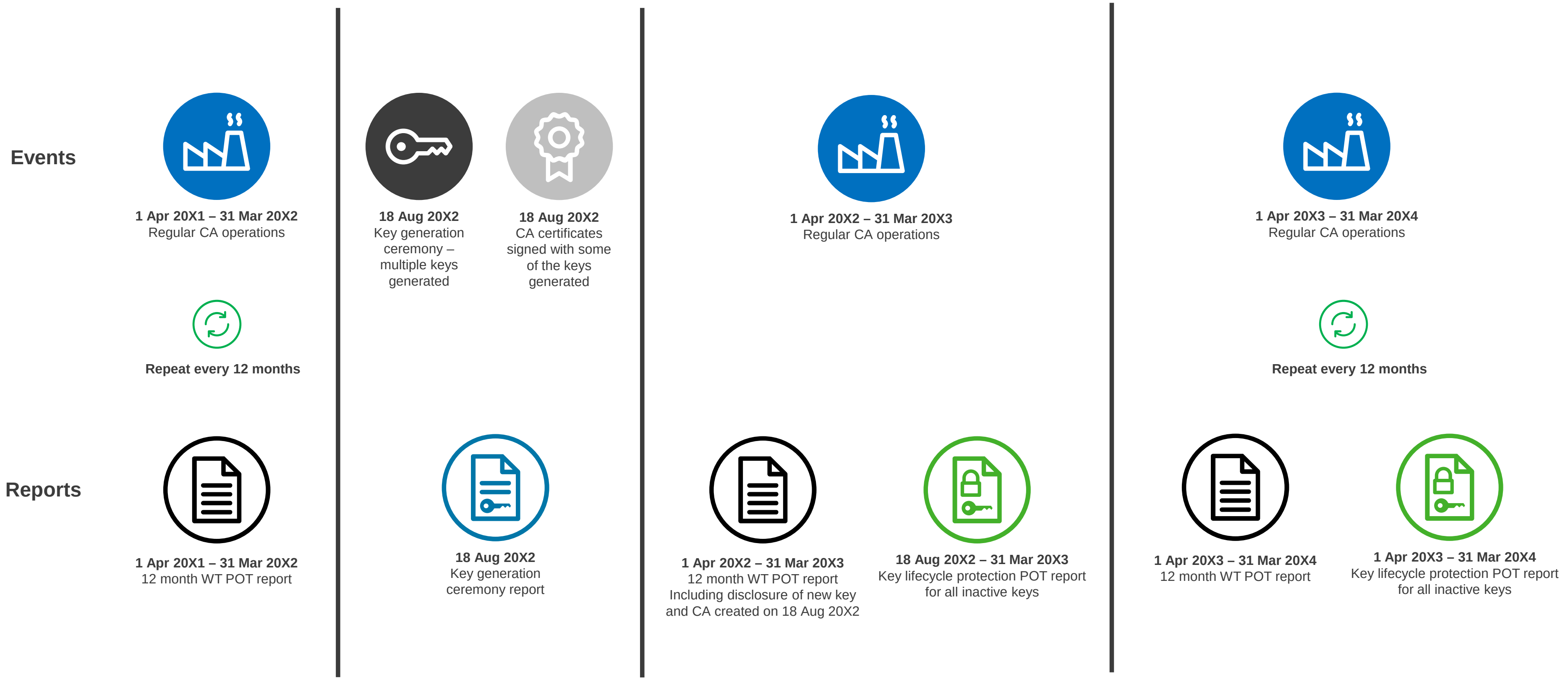
1 Apr 20X1 – 31 Mar 20X2
12 month WT POT report

18 Aug 20X2
Key generation ceremony report

1 Apr 20X2 – 31 Mar 20X3
12 month WT POT report
Including disclosure of new key and CA created on 18 Aug 20X2

1 Apr 20X2 – 31 Mar 20X3
12 month WT POT report

Scenario 5: Existing CA, additional key generation during the period with some parked keys for future use



Events	**1 Apr 20X1 – 31 Mar 20X2** Regular CA operations **Repeat every 12 months**	**18 Aug 20X2** Key generation ceremony – multiple keys generated **18 Aug 20X2** CA certificates signed with some of the keys generated	**1 Apr 20X2 – 31 Mar 20X3** Regular CA operations	**1 Apr 20X3 – 31 Mar 20X4** Regular CA operations **Repeat every 12 months**
Reports	**1 Apr 20X1 – 31 Mar 20X2** 12 month WT POT report	**18 Aug 20X2** Key generation ceremony report	**1 Apr 20X2 – 31 Mar 20X3** 12 month WT POT report Including disclosure of new key and CA created on 18 Aug 20X2 **18 Aug 20X2 – 31 Mar 20X3** Key lifecycle protection POT report for all inactive keys	**1 Apr 20X3 – 31 Mar 20X4** 12 month WT POT report **1 Apr 20X3 – 31 Mar 20X4** Key lifecycle protection POT report for all inactive keys

Other Event Reports

- Event reports - completed
  - key generation,
  - key protection,
- Event reports – in process (being reviewed)
  - transport,
  - migration
  - destruction

to cover all expected events cradle to grave

Enhancement of CPA Canada Processes

CPA Canada is revamping processes with an aim 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
- 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	Daniel Adam	Deloitte
Chris Czajczyc	Deloitte	Tim Crawford	BDO
Donoghue Clarke	EY	Zain Shabbir	KPMG
David Roque	EY	Santhan Raj	KPMG
Eric Lin	EY	Matt Jantzen	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?