Standardization for Digital Credentials and Digital Trust Services

4th Digital Transformation in Government Conference

June 15, 2023

Standards Council of Canada
Open a world of possibilities.

Conseil canadien des normes
Un monde de possibilités à votre portée.

Canada

Agenda

- National Standardization System
- SCC’s role
- Government of Canada Perspective
- Project Overview
- National Technical Specification Overview
- Pilot Overview
- Observation Committee Members Roles and Responsibilities

What is SCC's mandate and role?

Standards Council of Canada's Roles

- National Standards Body
- National Accreditation Body
- F/P/T government engagement and support

Standardization refers to

- Voluntary Consensus Standards
- Conformity Assessment

The National Standardization System Partners:

- Standards Development Organizations
- Conformity Assessment Bodies
- Thousands of volunteer experts, public and private sectors

How can standards and conformity assessment help?

Third-party trust infrastructure that serves private and public needs alike

- E.g., knowing which wallets can be trusted

Voluntary consensus standard that

- reflects the broadest possible set of interests
- contains certification criteria
- is developed transparently according to international and national standards development good process

Conformity assessment that

- follows international and national requirements for consistency, fairness, and transparency

Government of Canada Perspective

- Intention is to only allow certified digital trust services to be used within federal jurisdiction (e.g., only certified digital wallets could be used to obtain Government of Canada services using digital credentials)
- Standardization of digital credentials and digital trust services is needed to:
  - Ensure digital credentials and digital trust services are interoperable, so they can be seamlessly used across Canada and with trading partners.
  - Make it easier for individuals and organizations to know which digital credentials and digital trust services they can trust.
  - Enable individuals and organizations to use the trusted wallet of their choice across Canada and with trading partners.
  - Enable innovation and fair competition in the digital credential space.
  - Support the federal government's approach of testing and maturing the products of innovative companies to establish enterprise-grade infrastructure and enabling services.

Project Overview

Phase		Outcomes
Phase 1	Create a Standardization Landscape	Identify Canadian and international standards and conformity assessment tools
Phase 2	Develop a Technical Specification	Deliver open, stakeholder-driven requirements for trust and interoperability
	Develop a prototype conformity assessment program	Pilot to provide useful information for all stakeholders
Phase 3	Pilot the prototype conformity assessment program	Test the Technical Specification to access stakeholder impact
Phase 4	Develop full-scale Conformity Assessment Program	Incorporate lessons-learned and develop program that meets overall project goals

Phase 1: Create a Standardization Landscape

- **Lead: SCC**
  - Developed a standards landscape, including:
    - comprehensive search using keywords
    - data synthesis of thousands of standards
    - analysis of findings
    - drafting of recommendations

- **Stakeholder: Government of Canada (ISED)**
  - Provided background information

Phase 2: Develop Technical Specification and Prototype Conformity Assessment Program

- **Lead: SCC**
  - Managed project and contracting
- **Supplier: CIO Strategy Council** (now Digital Governance Council)
  - Developed technical specification
- **Stakeholders: Technical Committee**
  - Wrote the technical specification
    - 10 federal department and agencies
    - 8 provincial government organizations from 5 provinces
    - 2 municipalities
    - 62 subject matter experts

Phase 2: Develop Technical Specification and Prototype Conformity Assessment Program

Outcomes

- Drafting - May 13, 2021 to January 9, 2023
- Public review - January 9 to February 3, 2023
- Public review results
  - 1868 views
  - Approx. 290 comments from 30 individuals or organizations:
    - 8 Canadian government (7 federal, 1 provincial)
    - 12 Industry/Users (6 Canadian, 6 foreign)
    - 2 Academia (1 Canadian, 1 foreign)
    - 4 General Interest (3 Canadian, 1 foreign)
    - 4 Anonymous

Overview of the National Technical Specification

- Intended to be technology framework agnostic, including being flexible enough to support W3C Verifiable Credentials, Mobile driving licence (mDL) and other approaches
- Includes conformance requirements for the following digital trust services:
  - Issuer Component
  - Holder Component (e.g., digital wallet)
  - Verifier Component
  - Digital Trust Registry Component
- Examples of privacy-related requirements:
  - 10.1.5 The Holder Component shall enable the Holder to manage privacy and sharing settings.
  - 10.1.6 The Holder Component shall enable the Holder to control the sharing of digital credential data, in whole, in part or as a derivation, and should encourage the Holder to avoid oversharing data.
    NOTE: Selective disclosure is an example of what is covered in this context by “in part, or as a derivation”.
  - 10.1.21 The Holder Component shall request Holder authorization before sharing digital credential data.
  - 10.1.22 The Holder Component shall request Holder authorization before accepting, declining, or removing digital credentials.

Overview of the National Technical Specification (cont'd)

- Examples of security-related requirements:
  - 7.1.1 Data shall be encrypted using a Cryptographic Module Validation Program – certified encryption module.
  - 7.1.3 Data-in-transit protection shall be provided using TLS 1.2, or subsequent versions.
  - 7.1.4 Cryptographic algorithms shall be compliant with the recommendations for Protected B information in the CSE publication Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information and Guidance on Securely Configuring Network Protocols (ITSP.40.111 and ITSP.40.062).
  - 10.1.7 The Holder Component shall use shared secret (e.g., passwords, passphrases, PINs) or biometric authentication to prevent unauthorized access.
- Examples of other user-interface requirements:
  - 9.1.20/10.1.23/11.1.7 The Issuer/Holder/Verifier Component shall provide support for English and French, and should provide support for additional languages (e.g., Indigenous languages).
  - 9.1.21/10.1.7/11.1.8 The Issuer/Holder/Verifier Component shall conform to the Harmonized European Standard on Accessibility requirements for ICT products and services (EN 301-549)

(Apr. 2023 to Jan. 2024)

Phase 3: Pilot the Prototype Conformity Assessment Program

- **Lead: SCC**
  - Design and manage the conformity assessment pilot program, and develop lessons learned report
- **Stakeholders:**
  - **Product developers:** Products can be submitted for pilot certification.
  - **Conformity Assessment Bodies:** Carry out pilot certification to the technical specification.
  - **Observation Committee:** Public and private sector forum for learning and information sharing.

(Oct. 2023 to May 2025)

Phase 4: Develop Full-Scale Conformity Assessment Program

- **Lead: SCC**
  - Project management
  - RFP for National Standard of Canada (NSC)
  - Development of the full-scale conformity assessment program
- **Stakeholders:**
  - **Government:** help write the NSC and evaluate use of the accreditation scheme for regulatory and policy objectives
  - **Standards Development Organization:** develops the NSC
  - **Experts / interested parties:** join the technical committee to develop the NSC
  - **Conformity Assessment Bodies:** get accredited to perform certification to the NSC

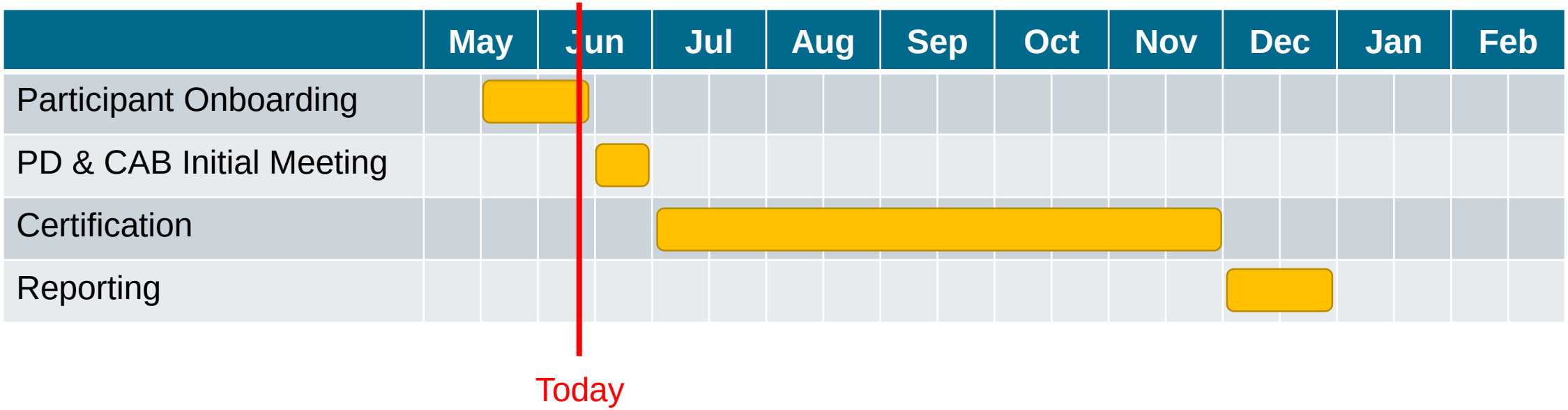
Pilot Overview

Goal: Understand the impact of DGSI/TS 115 Technical Specification for Digital Credentials and Digital [illegible] Services

Output: Lessons Learned Report to inform the development of a National Standard of Canada and a full-scale accreditation program

Participants	Role	Responsibilities
Conformity Assessment Bodies	Carry out certification	• Take on 1 to 3 products for certification • Act under confidentiality agreements with Product Developers • Report regularly to SCC any challenges and opportunities
Product Developers	Submit products for certification	• Work with a CAB to demonstrate conformity with DGSI/TS 115 • Report regularly to SCC any challenges and opportunities
Observation Committee	Observe, learn, and comment on pilot proceedings	• Discuss summary information about the pilot • Contribute to the lesson's learned report

Pilot Timeline



Upcoming Opportunities

Observation Committee (Jun. to Dec. 2023)

- Monthly meetings for 5 to 7 months
- Meeting times will alternate morning and late afternoon to accommodate international schedules
- Pilot summary information will be shared for review ahead of each meeting
- Specific questions forwarded by the TS expert drafting team
- Product developers or conformity assessment bodies may present to the observation committee
- Microsoft Teams will be used for information sharing and discussion between meetings

Phase 4 Technical Committee (Call-out in Fall 2023)

- Led by an SCC-accredited Standards Development Organization
- Members will review the TS and pilot learnings and help draft the National Standard of Canada

Thank you

Questions?

accreditation@scc.ca