Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Canada

Standardization of Digital Credentials and Digital Trust Services

Government of Canada Overview and Q&A Session for the W3C Credentials Community Group

January 23rd, 2023

Vision:

Services can be obtained quickly and easily across Canada and trading partners, using safe and secure Digital Credentials

Digital Credentials would be:

- Optional: Digital credentials are completely voluntary. Other forms of physical documents, like a driver's license or passport, would still be used.
- Convenient: You would be able to access services faster using a variety of digital platforms (mobile phones, laptops, tablets, etc.).
- Secure: You and your digital credentials would benefit from Canada's strong and ever evolving cyber security protections.
- Private: You would be able to choose who sees your information, and what they get to see, with only the required data being disclosed. Digital credentials would keep your private information private and give you more control over your information.
- Accessible: Your digital credentials would work with assistive technology and reduce challenges associated with paper forms and in-person visits.

Digital Credentials would not be:

- Stored in a central database: Digital credentials would be stored on your personal device(s) and by the organization that issues the credential, just as they are done today.
- A surveillance tool: Government and organizations will not know where you have been or where you have used your digital credentials.
- Usable without your consent

Credentials are issued by the public and private sector in Canada

Federal Government issues documents such as Certificate of Indian Status, citizenship and immigration documents, passports and federally-regulated licences and permits.

Provinces and territories issue documents such as birth certificates, driver licences, health cards and provincially-regulated licenses and permits.

Other public and private organizations issue documents such as educational qualifications, records of employment, certifications and proof of incomes.

Various levels of Canadian governments, including Indigenous governments and National Indigenous Organizations, and other public and private organizations issue important credentials that help individuals and businesses obtain and deliver services across Canada and borders

Why standardization is needed

Challenge: In Canada, there currently lacks alignment on how to verify or certify whether digital credentials and digital trust services meet interoperability, privacy and security requirements.

- Citizens and organizations are doing this independently, which is too burdensome for most and confusing for the market.
- Risks creating jurisdictional and sectoral silos, where users are forced to juggle many digital wallets and face many barriers to service.
- Risks creating an uneven playing field for solution providers and stifling market innovation, leading to platform capture and vendor lock-in.

Why standardization is needed (cont'd)

Goal: A National Standard of Canada and a full-scale conformity assessment program that is aligned with international best practices

- 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.

Overview of the project plan

- **Phase 1 (Winter 2020 to Spring 2021– Completed):** Landscape scan of national and international standards activities for digital credentials.
- **Phase 2 (Spring 2021 to Winter 2022):** National Technical Specification and Prototype Accreditation Program sets baseline requirements for interoperability and trust amongst digital credentials issuers, verifiers, and holders.
- **Phase 3 (Winter 2022 to Fall 2023):** Prototype Accreditation Program pilots the National Technical Specification and assesses stakeholder impact.
- **Phase 4 (Fall 2023 to Winter 2025):** Full-scale Conformity Assessment and Accreditation Program developed to incorporate lessons-learned and meet overall project goals.

Key next steps

- **January 9th to 27th, 2023:** Public review of the National Technical Specification
- **February 2nd Week:** Call for interest for the Prototype Accreditation Program, seeking conformity assessment bodies and developers of digital credentials and digital trust services to test certification of their products.
- **March 17th Week:** Publish the National Technical Specification
- **March 2023:** Develop Prototype Accreditation Program
- **Spring to Fall 2023:** Prototype Accreditation Program tests the National Technical Specification in a pilot certification process.

Opportunities to participate

Phase 2: Provide feedback through the public review for the National Technical Specification (from January 9th to 27th, 2023)

- News release announcing the public review
- Draft National Technical Specification (where feedback can be provided)

Phase 3: Participate in the Prototype Accreditation Program to test the National Technical Specification in a pilot certification process

- Conformity assessment bodies and developers of digital credentials and digital trust services can participate in pilot test certification of their products.
- Other organizations can participate on the observation committee to provide feedback on pilot outcomes.
- If you are interested in participating, please contact Standards Council of Canada Accreditation Services.

Phase 4: Participate in the development of National Standard(s) of Canada to address gaps identified during the public review and the pilot

- Supports the development of a Full-scale Conformity Assessment and Accreditation Program

Overview of the National Technical Specification

- Intended to be technology framework agnostic, including being flexible enough to support multiple technology frameworks for W3C Verifiable Credentials and Mobile driving licence (mDL)
- Includes objects of conformity for these digital trust services:
  - Issuer Component
  - Holder Component (e.g., digital wallet)
  - Verifier Component
  - Digital Trust Registry Component
- Also includes requirements for:
  - Digital Credentials (common requirements)
  - Storage
  - Cryptographic Module
  - Decentralized Identifier

Examples of Privacy-Related Requirements

10.1.8 The Holder Component shall be able to decline digital credentials from an Issuer.

10.1.12 The Holder Component shall be able to respond to a Holder's request to remove a digital credential and stop persisting that digital credential.

10.1.14 The Holder Component shall have a mechanism to create and submit a verifiable presentation to a relying party in response to:

a. A Holder action.
b. A request for a verifiable presentation from a Verifier, if approved by the Holder.

10.1.18 The Holder Component shall enable the Holder to manage privacy and sharing settings.

10.1.19 The Holder Component shall enable the user to control the sharing of digital credential data, in whole, in part, or as a derivation.

10.1.20 The Holder Component shall ensure there is Holder consent before sharing digital credential data and before accepting, declining, or removing digital credentials.

Examples of Security-Related Requirements

6.1.1 All data shall be protected during data-in-transit and data-at-rest in accordance with Section 7.

6.1.2 All data held in device-based or cloud-based storage shall be encrypted in accordance with Section 7 of this Specification.

6.1.3 Cloud-based storage shall be implemented in accordance with ISO/IEC 27018 to protect personally identifiable information (PII) and ISO/IEC 29100 to protect personal information (PI).

7.1.1 Data shall be encrypted using a Cryptographic Module Validation Program – certified encryption module.

Note: Products validated as conforming to FIPS 140-1 or FIPS 140-2 (or soon FIPS 140-3) are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Protected Information (Canada).

7.1.3 Cryptographic algorithms shall be compliant with the recommendations for Protected B Information as outlined in the CSE publication Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information (ITSP.40.111).

7.1.4 The cryptographic module shall ensure support for quantum-safe cryptography using cryptographic algorithms, cryptographic parameter sizes, key lengths and crypto periods which are configurable and which can be updated within protocols, applications and services to consistent with transition guidance in time to meet specified transition dates.

10.1.2 The Holder Component shall use password or biometric authentication to prevent unauthorized access.

a. The Holder Component should encourage the use of passwords that are in accordance with Best practices for passphrases and passwords (ITSAP.30.032).
b. The Holder Component shall limit the number of unsuccessful authentication attempts without negative consequences (e.g., suspending access to the Holder Component or wiping the contents of the Holder Component).
c. The Holder Component shall require re-authentication after being idle for a period of time, with that period of time being configurable by the Holder.
d. The Holder Component may support the ability to remotely allow, suspend or restore access to the Holder Component.

11.1.4 The Verifier Component shall determine whether the Holder has demonstrated control over a digital credential by means of one or more authenticators.

12.1.2 The Digital Trust Registry Component shall employ adequate authentication and access control to prevent against unauthorized access, compromise, or destruction of data.

Examples of Other User Interface Requirements

9.1.14 The Issuer Component shall notify the Holder of any changes to digital credential information.

9.1.33 The Issuer Component shall inform the Holder of the change in digital credential status

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)

9.1.31 The Issuer Component should provide to the Holder the ability to revoke a digital credential issued to the Holder.

10.1.16 The Holder Component shall be able to manage connections (e.g., to Issuers, requesting parties, and other parties) in accordance with Section 7 requirements.