National Standard of Canada
Standards Proposal

Proposed Standard Title:
Digital Trust and Identity - Techniques – Code of Practice

Plain Language Summary of Standards Proposal (200 words max):
As work in the Digital Trust and Identity series continues at an accelerated pace, there has been a need identified to support the normative work with a document that can offer the user informative references and support material, best practices, and codes of practice.

Proposed Scope:
This document provides a reference set of generic digital trust, identity, credentials and wallets techniques including implementation guidance. This document is designed to be used by organizations: a) within the context of a digital trust and identity management system based on the CAN/CIOSC 103 series of standards; b) for implementing digital trust and identity programs based on internationally recognized best practices; and c) for developing organization-specific digital trust and identity guidelines. This standard applies to all organizations, including public and private companies, government entities, and not-for-profit organizations. NOTE: This document is not intended for conformity assessment.

Strategic Need:

Identify the strategic need of key stakeholders and confirmation expressing the need.

This includes consideration for:

- *a. The strategic need of key stakeholder (e.g. legislator, industry, government, consumers);*
- *b. The type of standard (international, regional, domestic standards and harmonization need);*
- *c. Addressing up-to-date vs outdated standard to ensure latest innovative/technology/safety features available for businesses;*
- *d. If the standard is intended to support national/regional/international certification programs;*
- *e. If there is stakeholder intention to transition to different standard;*
- *f. The type of maintenance (periodic, continuous, stabilized, best before date); and*
- *g. The use of "CAN" descriptor.*

As the digital trust and identity ecosystem continues to evolve at a rapid pace, there is a clear need for Standards and guard rails to assist users in developing and demonstrating trust in their programs. As these Standards continue to develop, there is a need to support this work and provide the users with assistance in developing, implementing, and deploying their digital trust and identity programs.

This techniques and code of practice document aims to offer the user industry techniques and guidance to ensure the user is implementing a program that is aligned and interoperable with international best practices.

This document not only intends to offer support for users looking to deploy the CAN/CIOSC 103 series of Standards, but any user looking to develop and deploy a digital trust and identity program at their organization.

This proposed National Standard of Canada will:

- be maintained on a periodic basis as determined by the technical committee responsible for developing the standard; and
- use the CAN descriptor.

Need for Availability in Both of Canada's Official Languages: *Do stakeholders need the standard published in both official languages?* *Do users of the standard need the standard published in both official languages?* *Do authorities having jurisdiction need the standard published in both official languages?* *Are there health and safety related needs for the standard to be published in both official languages?* *For adoptions, is there availability of the regional/international standard or other deliverable from the source?* *For adoptions, is there an agreement with the source committee to facilitate official translation?*	YES

Geographical Representation Considerations: *Identify the Canadian geographical representation appropriate to the subject area covered by the standard.* *Geographic representation may consider factors such as:* *a. Industry (e.g. petroleum in petroleum producing provinces);* *b. Reference in regulation (if a regulation exists in a province); or* *c. Commodity characteristics and social impact (e.g. heating oil for northern climates).*
All sectors of the economy.

Trade:

Identify how the standard meets the needs of the marketplace and contributes to advancing trade in the broadest possible geographical and economic contexts.

For example:

a. *Facilitate Canadian innovation to lead internationally;*
b. *Support the objectives of "One standard, one test, accepted everywhere";*
c. *Support the objectives of "First to Market"; or*
d. *Foster international/ regional/ national alignment of requirements.*

Alignment and interoperability are core fundamentals of an effective digital trust and identity program. By developing and offering a key document that incorporates industry and international best practice, Canadian organizations will ensure that their digital trust and identity programs are effective, aligned and interoperable both domestically and internationally.

Relevant existing documents at the international, regional and national level:

- CAN/CIOSC 103-1:2020: Digital trust and identity -- Part 1: Fundamentals
- CAN/CIOSC 103-2: 2021: Digital trust and identity -- Part 2: Delivery of Healthcare Services
- Australia Trusted Digital Identity Framework
    - https://www.dta.gov.au/our-projects/digital-identity/join-identity-federation/accreditation-and-onboarding/trusted-digital-identity-framework
- ITSP.30.031 User Authentication Guidance for Information Technology Systems
    - https://www.cse-cst.gc.ca/en/node/2454/html/28582
- Public Sector Profile of the Pan-Canadian Trust Framework
    - https://canada-ca.github.io/PCTF-CCP/
- Treasury Board Secretariat of Canada. Directive on Identity Management. 2019.
- Treasury Board Secretariat of Canada. Guideline on Identity Assurance. 2016.
- Treasury Board Secretariat of Canada. Guideline on Defining Authentication Requirements. 2012.
- DIACC P1000 Series, Pan-Canadian Trust Framework.
- European Union. Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market. 2014.
- ISO/IEC 24760-1:2019, IT Security and Privacy -- A framework for identity management -- Part 1: Terminology and concepts
- ISO/IEC 24760-2:2015, Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements
- ISO/IEC 24760-3:2016, Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice
- ISO/IEC 29115:2013, Information technology -- Security techniques -- Entity authentication assurance framework
- ISO/IEC 29100 Information Technology – Security Techniques – Privacy Framework
- ISO/IEC 27018 Information Technology – Security Techniques – Code of Practice for Protection of PII in Public Clouds Acting as PII Processors
- New Zealand Digital Identity
    - Evidence of Identity Standard
    - Authentication Standards
    - Identification Management
    - https://www.digital.govt.nz/standards-and-guidance/identity/digital-identity/

- NIST Special Publication 800-63 Series, Digital Identity Guidelines
- GPG 44 Authentication Credentials in Support of HMG Online Services
- GPG 45 Identity Proofing and Verification of an Individual
- GPG 43 Requirements for Secure Delivery of Online Public Services
- GPG 53 Transaction Monitoring for HMG Online Service Providers