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

Canada

Pan-Canadian Trust Framework

Overview

23 February 2021
Version 0.1

GCDOCS#TBD

Outline

1. What is digital identity?
   a. What are some of the common ways of identifying someone electronically?
   b. Does Canada have a digital ID system?
2. What is the Pan-Canadian Trust Framework?
   a. What is it? What is a “trust framework”?
   b. What is its purpose?
   c. How does it accomplish that?
   d. What are examples of it being currently used?
   e. All of this is public sector, what about private sector?
3. Are there any recommendations for PHAC context?

What is a Trusted Digital Identity?

What is it?

***A trusted digital identity** is an electronic equivalent of who you are as a real person, used exclusively by you, to receive valued services and to carry out transactions with trust and confidence.*

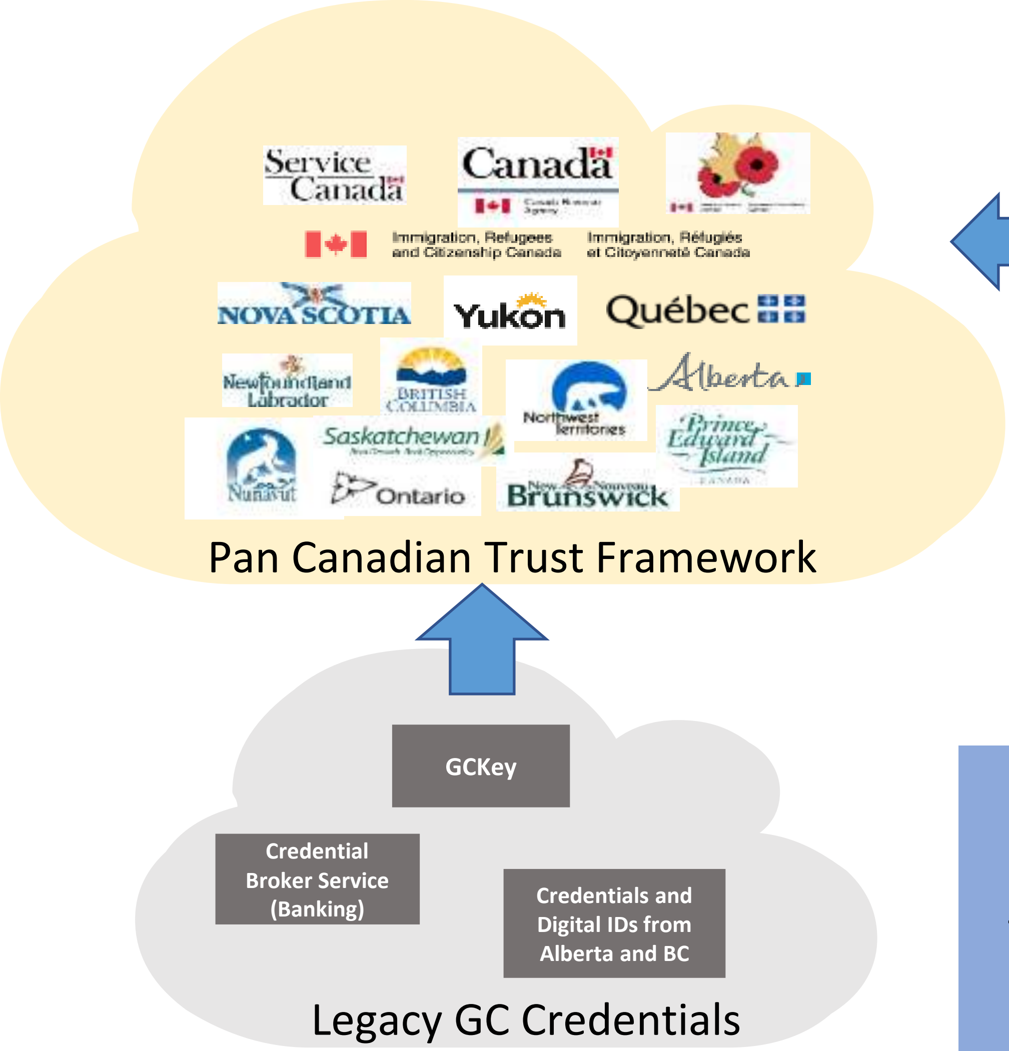
Trusted Digital Identity confirms that 'you are who you say you are' in an digital context.

Why does it matter?

Digital Identity is the foundation to moving more services online, where our citizens expect to be.

- **Digital identities** of persons and organizations; and
- **Digital relationships** between persons, between organizations, and between persons and organizations.

Canada’s Digital Identity Vision



Service Canada

Canada

Canada Revenue Agency

Immigration, Refugees and Citizenship Canada

Immigration, Réfugiés et Citoyenneté Canada

NOVA SCOTIA

Yukon

Québec

Newfoundland Labrador

BRITISH COLUMBIA

Northwest Territories

Alberta

Nunavut

Saskatchewan

Ontario

New Nouveau Brunswick

Prince Edward Island CANADA

Pan Canadian Trust Framework

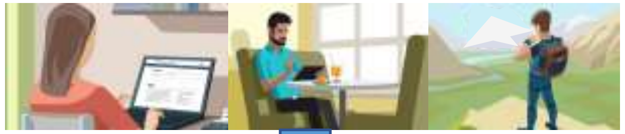
GCKey

Credential Broker Service (Banking)

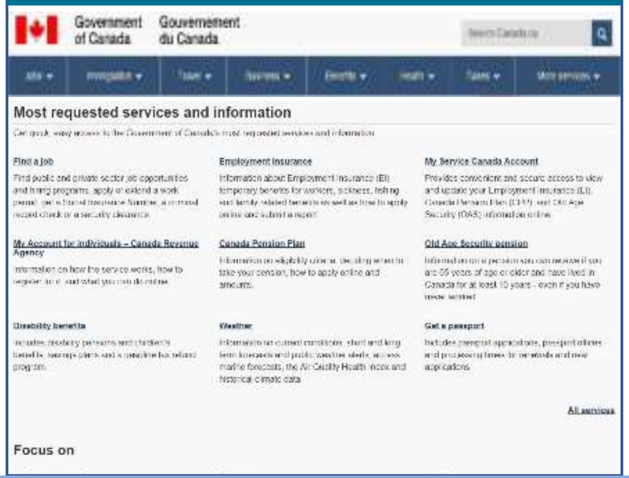
Credentials and Digital IDs from Alberta and BC

Legacy GC Credentials

Trusted



Sign In Canada



Most requested services and information

Get quick, easy access to the Government of Canada's most requested services and information

Find a job

Find public and private sector job opportunities and hiring programs, apply or extend a work permit, get a Social Insurance Number, a criminal record check or a security clearance.

Employment Insurance

Information about Employment Insurance (EI) temporary benefits for workers, sickness, fishing and family related benefits as well as how to apply online and submit a report.

My Service Canada Account

Provides convenient and secure access to view and update your Employment Insurance (EI), Canada Pension Plan (CPP) and Old Age Security (OAS) information online.

My Account for Individuals – Canada Revenue Agency

Information on how the service works, how to register for it, and what you can do online.

Canada Pension Plan

Information on eligibility criteria, deciding when to take your pension, how to apply online and amounts.

Old Age Security pension

Information on a pension you can receive if you are 65 years of age or older and have lived in Canada for at least 10 years - even if you have never worked.

Disability benefits

Includes disability pensions and children's benefits, savings plans and a disability tax credit program.

Weather

Information on current conditions, short and long term forecasts and public weather alerts, access marine forecasts, the Air Quality Health Index and historical climate data.

Get a passport

Includes passport applications, passport offices and processing times for renewals and new applications.

All services

Focus on

Secure

Employment and Social Development Canada

Immigration, Refugees and Citizenship Canada

Innovation, Science and Economic Development Canada

Canada Revenue Agency

Veterans Affairs Canada
Anciens Combattants Canada

The Government of Canada is enabling a digital identity ecosystem for the nation, to be leveraged by all GC departments and agencies, other jurisdictions in Canada (provinces, territories, municipalities) and Canadian partners (private sector & other countries), to deliver services and issue digital identities to Canadians so they can access services seamlessly, anytime, anywhere and on any device.

Why a trust framework?

- In a federated model we are not centralizing information into a single source, rather we look to recognize the identities/credentials issued by partners
- Said another way, our focus is on assessing the trustworthiness of the issuer of identities/credentials
- A trust framework is an agreed upon method to assess the parties in the ecosystem and establish trust
- Enables a technology-agnostic assessment of a program/provider with regards to its ability to provide a trusted digital identity without vendor or techhology ‘lock-in.’

The Pan-Canadian Trust Framework

The PCTF is a model that consists of a set of agreed-on concepts, definitions, processes, conformance criteria, and an assessment approach.

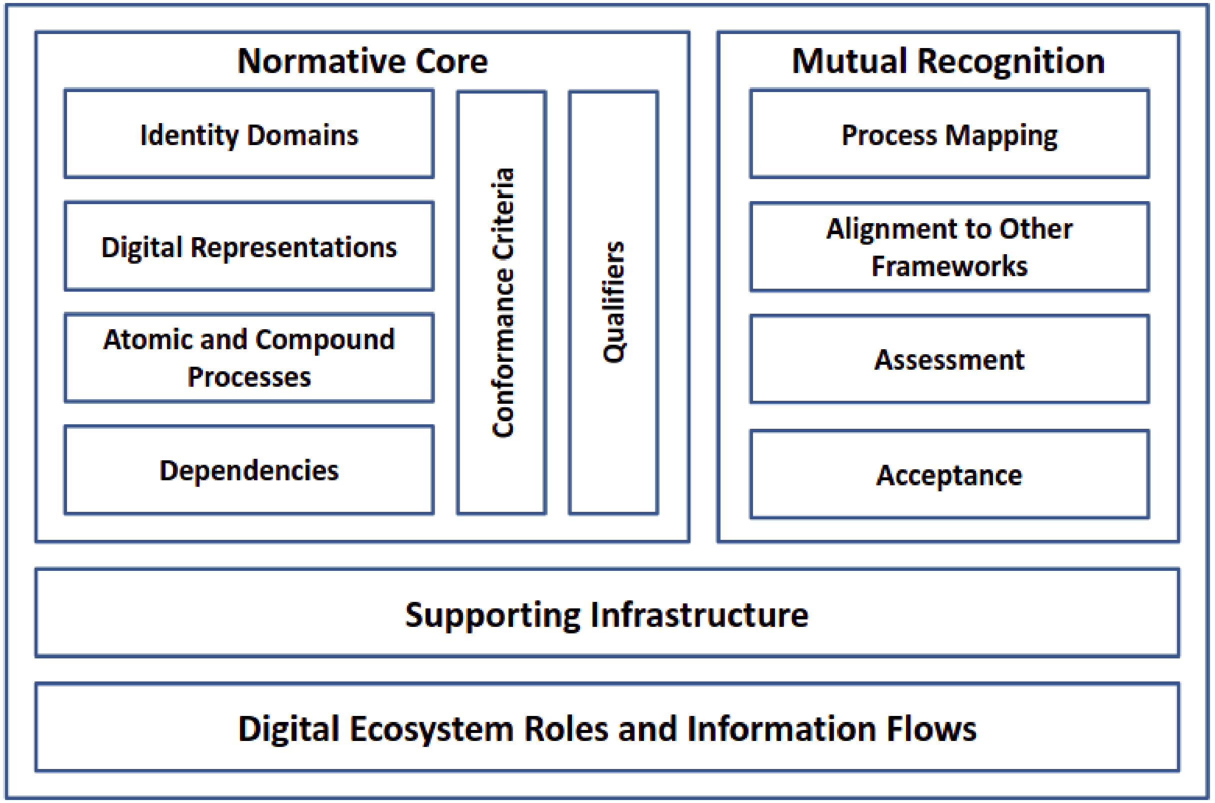
- A framework that relates and applies existing standards, policies, guidelines, and practices, and where such standards and policies do not exist, specifies additional criteria.

- The role of the PCTF is to complement existing standards and policies such as those concerned with security, privacy, and service delivery.

- Facilitates a common approach between the public sector and the private sector.

- Ensures alignment, interoperability, and confidence of digital identity solutions that are intended to work across organizational, sectoral, and jurisdictional boundaries. In addition, the PCTF supplements existing legislation, regulations, and policies.

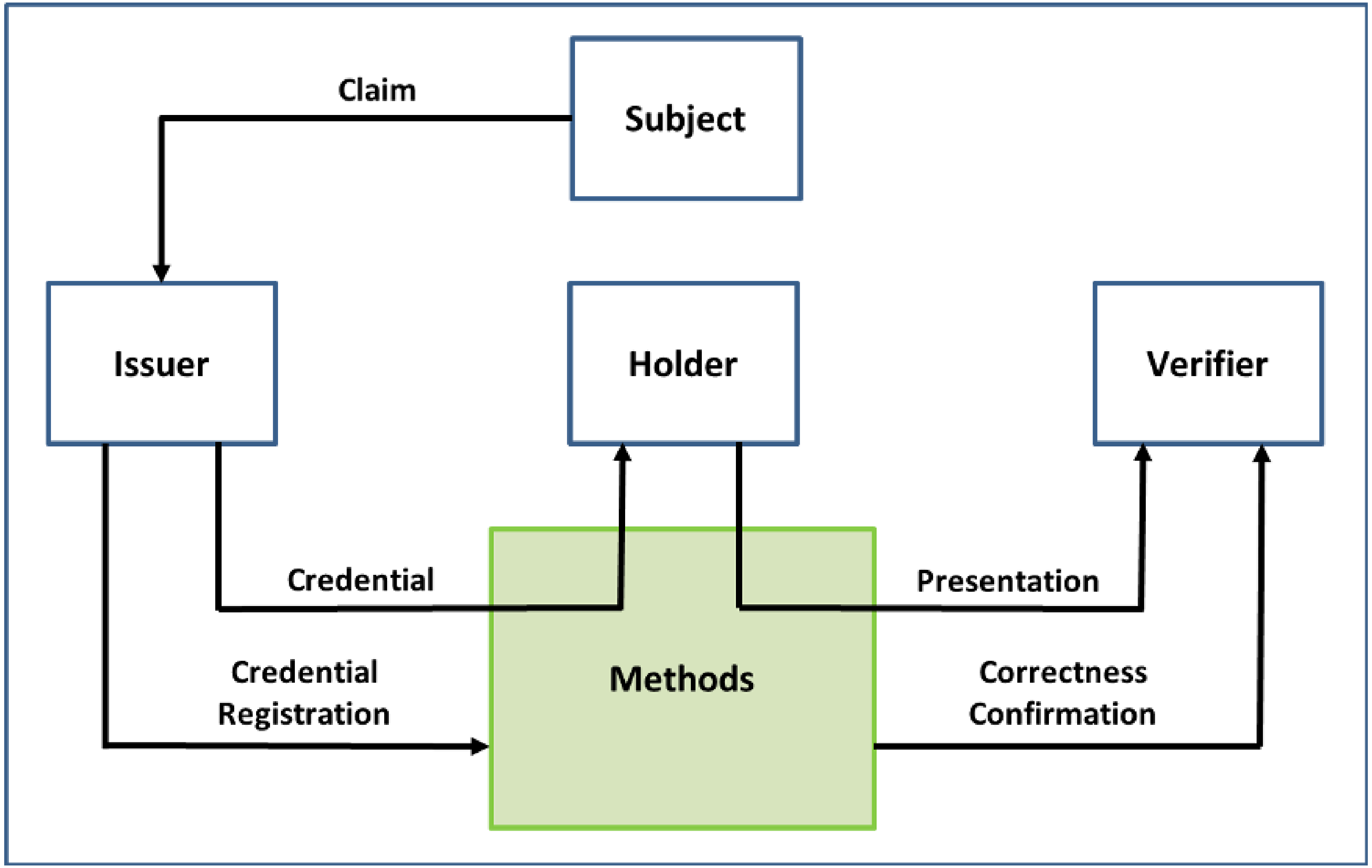
Pan-Canadian Trust Framework (Rules of the Road)



https://canada-ca.github.io/PCTF-CCP/

- A **Normative Core** component that encapsulates the key concepts of the PCTF;
- A **Mutual Recognition** component that outlines the current methodology that is used to assess and certify actors in the digital ecosystem;
- A **Supporting Infrastructure** component that describes the set of operational and technical policies, rules, and standards that serve as the primary enablers of a digital ecosystem; and
- A **Digital Ecosystem Roles and Information Flows** component that defines the roles and information flows within the digital ecosystem.

Digital Ecosystem – Roles & Information Flows



Pan-Canadian Trust Framework Assessment Approach

1. Pan-Canadian Trust Framework Document

- Comprehensive document (83 pages)
- Combines scope of **Persons, Organizations**, and **Relationships**
- Defines 29 **Atomic Processes and Qualifiers** (levels of assurance, etc.)
- Provides background information, high-level guidance and definitions.

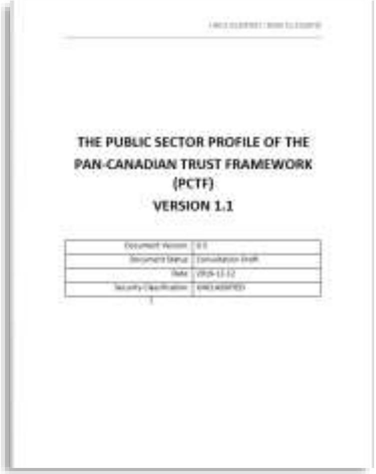
2. PCTF Assessment Worksheet

- Specifies **Conformance Criteria** for each atomic process (approximately 400+ in total)
- Outlines an **Overall Assessment Approach** to collect and assess evidence (program documentation, etc.)
- Documents assessment outcome for each conformance criteria: [**Accepted, Not Accepted, Accepted with Condition, Accepted with Observation, Not Applicable**]

3. GC Letter of Acceptance

- Formally documents the outcome of PCTF assessment process
- Issued to acknowledge acceptance of a trusted digital identity.

Primary Deliverable



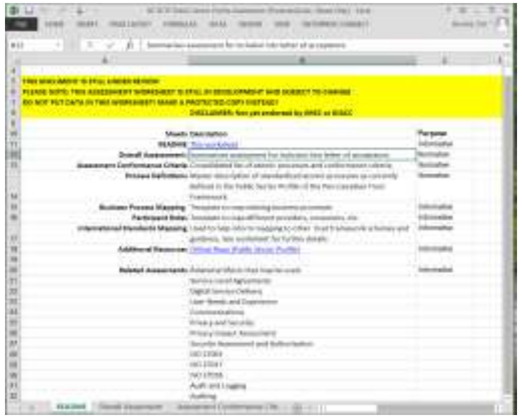
THE PUBLIC SECTOR PROFILE OF THE
PAN-CANADIAN TRUST FRAMEWORK
(PCTF)
VERSION 1.1

Document Version	[illegible]
Document Status	Consultation Draft
Date	[illegible]
Security Classification	UNCLASSIFIED

Consultation

GitHub

Assessment Worksheet



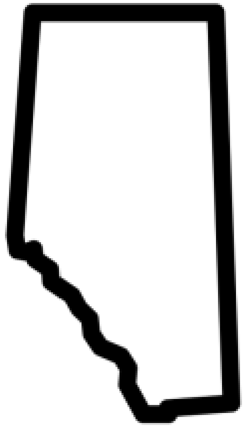
Sheets	Description	Purpose
README	[illegible]	[illegible]
Overall Assessment	[illegible]	[illegible]
Assessment Conformance Criteria	[illegible]	[illegible]
Process Definitions	[illegible]	[illegible]
Business Process Mapping	[illegible]	[illegible]
Participant Roles	[illegible]	[illegible]
International Standards Mapping	[illegible]	[illegible]
Additional Resources	[illegible]	[illegible]
Related Assessments	[illegible]	[illegible]

Acceptance

Trusted Digital Identity

Available at: https://github.com/canada-ca/pctf-ccp

PCTF Public Sector Profile Assessments: Conducted to Date



Province of Alberta

- **April-August 2018** Initial Assessment
- **September 2018:** Letter of Acceptance Issued
- **August 2019:** Go-Live on My Service Canada Account
- **Feb 2021:** Reassessment and framework agreement

Province of British Columbia

- **August-December 2019** Initial Assessment
- **Q1 2020:** Letter of Acceptance Issued (Jan 2020)
- **Q1 2020:** Go-Live on My CRA Login (Feb 2020) My Service Canada Account

Rest of Canada

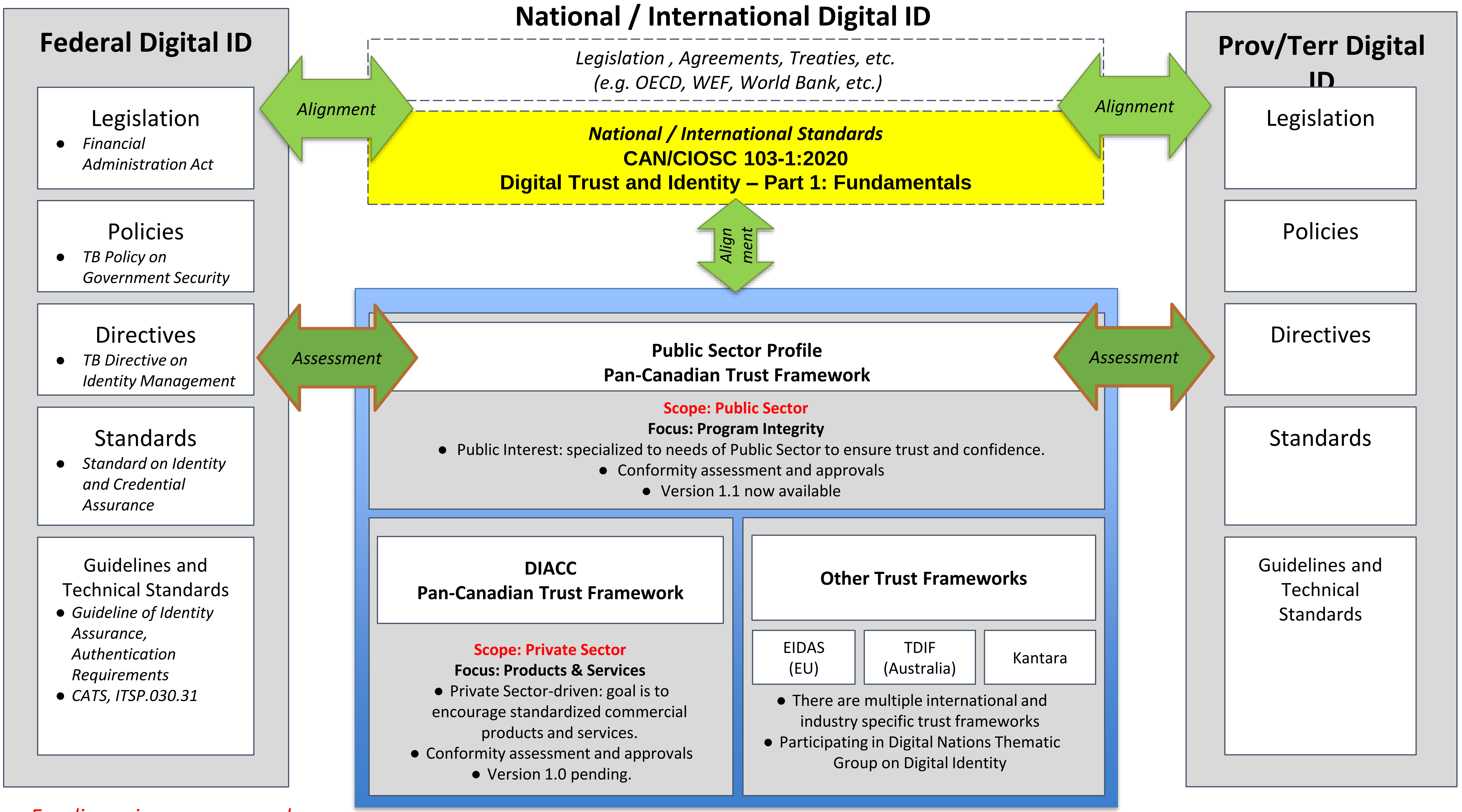
- **2021-202X (Est.)**

Open Short Link (tbs-sct.gc.ca)

Implementation Considerations for Vaccination Systems

Guiding Principles	Description
Focus on the user needs	• Trust and adoption are key. It should be up to citizens as to which format is most convenient for them.
Open standards-based approach	• The solution should be based on technology agnostic, open standards-based and with a nationally coordinated approach. • Open standards for data models and protocols are essential in order to maximize our chance for global interoperability, to avoid vendor lock-in, and to ensure transparency. • A focus on open standards-based credentials which will give provinces the option of having their own app if they wish.
Implement a decentralized approach (e.g. users having their own certificates in digital wallets, issued by the appropriate public authorities)	• A decentralized model, based on verifiable credentials, scales well, does not require back-end integration between the system of record and the system verifying the vaccination status. Further, the credentials themselves are controlled by the subject (holder), need only contain the minimum personally identifiable information (PII) or personal health information (PHI). This is preferable to standing up a centralized database which would have significant privacy implications and pushback by Canadians. • A federated and decentralized identity model can be used to tap into and collaborate on a pan-Canadian scale. In this manner, the GC does not need to host the data, as that is not federal jurisdiction (health data), while providing horizontal governance.
Coordinated approach centrally in the federal government	• Supporting information systems should apply GC identity management policy and standards, specifically, the Treasury Board Directive on Identity Management. • GC needs to lead as the alternative would result in a patchwork of different (or competing) solutions across the country and make it difficult when it comes to cross-country mobility and international border crossing. • Ensure that we work together as a federal family on this – there are many related initiatives on digital trust, digital identity, etc. These all need to be coordinated (especially for proof of concept and potential procurement).
Enable Pan-Canadian Interoperability and alignment with GC enterprise direction	• For a pan-Canadian approach and the emerging digital ecosystem, the Public Sector Profile of the Pan-Canadian Trust Framework should be applied as well. This framework should be used to ensure a 'trusted' ecosystem is built/leveraged and will seamlessly work with digital IDs as we move forward.
Monitoring and alignment of ecosystems	• Continue monitoring international guidance that is available or being done, including activities with WHO, OECD, W3C, Digital Nations, etc. to ensure the GC solution will match and work with international entities. • There is a convergence underway of three separate ecosystems: 1) Mobile Drivers Licences – driven by AAMA/ISO, 2) Digital Travel Credentials (ePassports) driven by ICAO, and 3) Verifiable Credentials driven by W3C. The GC will need to support all three ecosystems and ensure their complementarity to one another and to prevent fragmentation of systems, or confusion by the user.

Annex



National / International Digital ID

Legislation , Agreements, Treaties, etc.
(e.g. OECD, WEF, World Bank, etc.)

National / International Standards
CAN/CIOSC 103-1:2020
Digital Trust and Identity – Part 1: Fundamentals

Federal Digital ID

Legislation
- *Financial Administration Act*

Policies
- *TB Policy on Government Security*

Directives
- *TB Directive on Identity Management*

Standards
- *Standard on Identity and Credential Assurance*

Guidelines and Technical Standards
- *Guideline of Identity Assurance, Authentication Requirements*
- *CATS, ITSP.030.31*

Prov/Terr Digital ID

Legislation

Policies

Directives

Standards

Guidelines and Technical Standards

Public Sector Profile
Pan-Canadian Trust Framework

Scope: Public Sector
Focus: Program Integrity
- Public Interest: specialized to needs of Public Sector to ensure trust and confidence.
- Conformity assessment and approvals
- Version 1.1 now available

DIACC
Pan-Canadian Trust Framework

Scope: Private Sector
Focus: Products & Services
- Private Sector-driven: goal is to encourage standardized commercial products and services.
- Conformity assessment and approvals
- Version 1.0 pending.

Other Trust Frameworks

EIDAS (EU) | TDIF (Australia) | Kantara

- There are multiple international and industry specific trust frameworks
- Participating in Digital Nations Thematic Group on Digital Identity

For discussion purposes only

CIO Strategy Council Digital Trust and Identity Standard: Overview

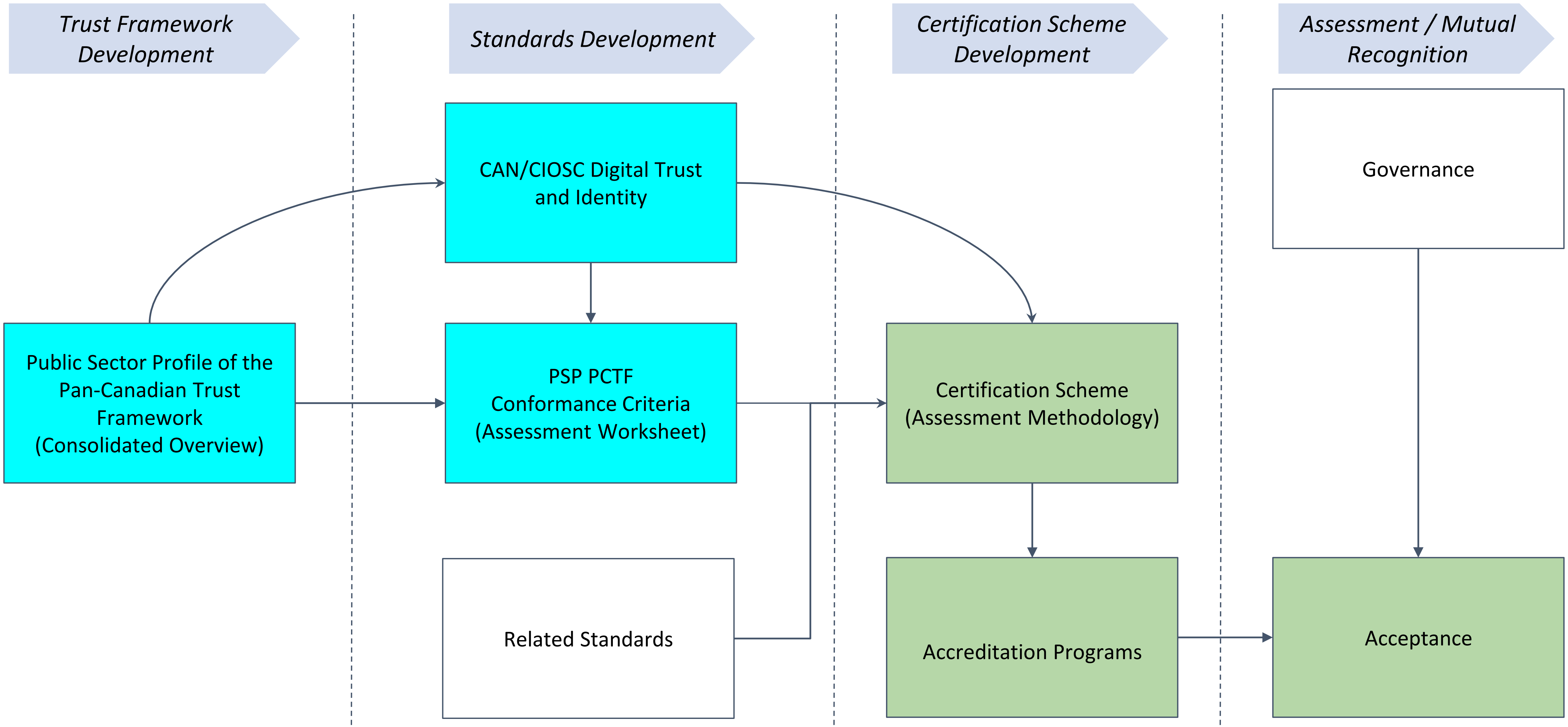
- **National voluntary standard** developed by the CIO Strategy Council technical committee on digital trust and identity and accredited by the Standards Council of Canada
- **Allows for the adoption of multiple trust frameworks -** PCTF, eIDAS, etc,
- **Specifies minimum requirements** and a set of controls for creating and maintaining trust in digital systems
- **Applies to all organizations**, including public and private companies, government entities, and not-for-profit organizations.
- **May be applied to either digital systems and services** that are used within an identity context, or to those that are used and applied across identity contexts i.e. in a credential and/or identity federation.

<u>Digital Trust and Identity</u>

1. **Introduction**
2. **Normative References**
3. **Terms and Definitions**
4. **Trust Framework**
    1. **Fundamentals**
    2. **Digital Identity Management**
5. **Processes**

Annexes (Normative)

Available at: https://ciostrategycouncil.com/standards/implement-standards/



Trust Framework Development

Public Sector Profile of the Pan-Canadian Trust Framework (Consolidated Overview)

Standards Development

CAN/CIOSC Digital Trust and Identity

PSP PCTF Conformance Criteria (Assessment Worksheet)

Related Standards

Certification Scheme Development

Certification Scheme (Assessment Methodology)

Accreditation Programs

Assessment / Mutual Recognition

Governance

Acceptance

- Joint Councils
- Subject Matter Experts

- CIO Strategy Council
- Standards Council of Canada
- Subject Matter Experts

- Scheme Owners
- Accreditation Bodies
- Subject Matter Experts

- Recognition Bodies
- Accredited Assessors
- Subject Matter Experts

Standards Alignment (Synopsis from Detailed Crosswalk Analysis)

- Highly-aligned and leverages content from the **Treasury Board Directive on Identity Management**, the **Standard on Identity Credential Assurance**, and the **Public Sector Profile of the Pan-Canadian Trust Framework**
- The Process definitions are identical to what is defined in the **Public Sector Profile of the PCTF,** with the following additions:
  - **Outcomes** based on Outputs defined in the PCTF
  - **Activities** - a more specific requirement detailing what activities must take place, but without getting into the detail of the conformance criteria.
- Fulfils the gap for a ‘national authority’ (albeit voluntary) for digital identity and trust frameworks.
- Similar in nature to the eIDAS regulation, and could evolve to become a federal or national regulation.
- Incorporates the ‘state of the art’ thinking contained in the Public Sector Profile of the Pan-Canadian Trust Framework and takes it one step further with additional high-level prescription of outcomes and activities.
- If adopted, this standard would:
  - encourage alignment between jurisdictions
  - accelerate the adoption of the Public Sector Profile of the Pan-Canadian Trust Framework
  - set the stage for mutual recognition of digital identities between countries (e.g., EU)