Conformity Assessment Scheme

Trusted Digital Identities for use by Public Sector Services

Scheme Author: CIO Strategy Council

Scheme Owner:

[Introduction 2](#_Toc2133680522)

[Background 3](#_Toc1703520500)

[References and Acknowledgements 3](#_Toc128712724)

[Scope of Scheme 4](#_Toc1295466717)

[Scheme Objectives 5](#_Toc623740809)

[Scheme Components 6](#_Toc22888877)

[Scheme Owner and Responsibility 6](#_Toc1460782087)

[Scheme Need 6](#_Toc642775430)

[Scheme Use 7](#_Toc1662487679)

[Assessment Methodology 7](#_Toc690733459)

[Objects of Conformity 8](#_Toc231402031)

[Conformity of Atomic Processes 8](#_Toc374324101)

[Conformity of Subject Entities 8](#_Toc1222483867)

[Conformity Assessment Qualifiers￼ 8](#_Toc240692368)

[Determining Scope of Assessment 9](#_Toc734463965)

[Marks 9](#_Toc1365050613)

[Digital Representations 9](#_Toc553228404)

[Identity Types 9](#_Toc494566526)

[Establishment and Maintenance of Identities 9](#_Toc1381151079)

[Trusted Digital Identity 11](#_Toc291588372)

[Conformity Assessment Activities 11](#_Toc933061728)

[Initial Conformity Assessment 11](#_Toc1825267138)

[Process Mapping 11](#_Toc1668399552)

[Assessment Methodology 12](#_Toc975502292)

[Atomic and Compound Processes 13](#_Toc957777920)

[Atomic Processes 13](#_Toc1788693447)

[Compound Processes 14](#_Toc1971943638)

[Dependencies 15](#_Toc1200496739)

[Conformity Assessment Criteria 15](#_Toc1420362307)

[Qualifiers 16](#_Toc1052018819)

[Additional References 16](#_Toc1851146868)

# Introduction

The purpose of this document is to define the conformity assessment scheme for Trusted Digital Identities for use by Public Sector Services.

The audience for this document includes:

* Business owners and program managers – to enable identity solutions in order to achieve business objectives or program outcomes.
* Regulatory and oversight bodies – to understand the implications on their role in the digital ecosystem; and
* Digital Identity technology and service providers – to understand where they fit in the digital ecosystem and to help define requirements for their products and services.

Definitions of various terms used in this document can be found in Appendix A: Terms and Definitions.

# Background

A conformity assessment scheme (‘scheme’) is used to demonstrate that specified requirements relating to a product, process, system, person, or body are fulfilled. Schemes can range from being voluntary, self-regulated for commercial marketing purposes, to mandatory schemes owned by certification bodies who are accredited, carried out by authorized independent assessors, and subject to normative and informative documents, such as national standards, related policies, and guidelines.

Within the Canadian context, this scheme is subject to the following

# References and Acknowledgements

**Normative References**

* CAN/CIOSC 103-1 Digital Trust and Identity: Fundamentals.

**Informative References**

* Public Sector Profile of the Pan-Canadian Trust Framework Version 1.4 (<https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_4)>

**Acknowledgements:**

This document contains information licensed under the **Open Government Licence – Canada.** Details of the licence can be found at: <https://open.canada.ca/en/open-government-licence-canada>

# Scope of Scheme

The scope of this scheme:

* Programs or business units that are accountable for issuing trusted digital identities for persons that are intended for use by public sector programs.
* Programs may be assessed in their entirety or as components that fit into a larger program context. This specified using the objects of conformity.

The scheme is technology-agnostic: it is defined in a way that allows for the assessment of different platforms, services, architectures, and technologies. The scheme does not recommend one technology solution over another.

The scope may include the following:

* **Persons in Canada:** all citizens and residents of Canada (including deceased persons) for whom an identity has been established in Canada.
* **Organizations in Canada:** all organizations registered in Canada (including inactive organizations) for which an identity has been established in Canada; and
* **Relationships in Canada:** of persons to persons, organizations to organizations, and persons to organizations.

# Scheme Objectives

## Scope of the Assessment

* Subset of scheme

# Scheme Components

## Scheme Owner and Responsibility

This scheme is jointly owned by:

* CIO Strategy Council
* Institute for Citizen-Centred Services
* ...

## Scheme Need

The identity management ecosystem in Canada is comprised of multiple trusted digital identity providers relying on authoritative source registries that span provincial/territorial and federal jurisdictions.

The market supports many ‘trusted digital identity providers’ for the purposes of commercial and personal purposes. There is a need, however. to certify a limited of trusted digital identity providers that can be used by persons to access high-value services, such as access to government benefits, or receiving authorizations or entitlements (e.g., license to drive).

The scheme enables the certification of trusted digital identity programs for the purposes of recognition and acceptance by public sector services. This includes:

* Trusted digital identities of entities: persons and organizations
* Trusted digital relations between entities (between persons, organizations, and between persons and organizations)

This scheme is for the certification of management systems with the purpose of providing trusted digital identities for use by public sector services.

This scheme is based on the Public Sector Profile of the Pan-Canadian Trust Framework (‘PSP PCTF’) to address the need to ensure the overall confidence of trusted digital identity programs that are technologically enabled by a variety of products and services.

The scheme enables the consistent assessment of trusted digital identity business processes through the definition of discrete process patterns (called atomic processes) that can be mapped that can be used for assessment purposes. This mapping enables assessors using the scheme to conduct a structured assessment, evaluate a identity solutions, identify dependencies on external organizations, and gaps that may existing.

The PCTF is technology-agnostic: it is defined in a way that allows for the use of different platforms, services, architectures, and technologies. The PCTF does not recommend one technology solution over another.

## Scheme Use

This scheme is intended to be used in conjunction with **IS0/IEC 17021:2015 Conformity Assessment Requirements for Bodies Providing Audit and Certification of Management Systems** to ensure that parties can rely of the certification of the management system (‘system’)/

This scheme is intended to be used for cases where there is a need to certify the performance of one or several of the following:

* Securely sign (authentication) into to portal applications, where core identity information may, or may not be required.
* Prove identity information that is required for to onboard or enrol (first-time registration) into high-value services.

This scheme has been developed in accordance with the following standards and guidelines

1. [Normative] **CAN/CIOSC 103-1:2020 Digital Trust and Identity – Part 1 Fundamentals** <https://ciostrategycouncil.com/standards/103_1_2020/>
2. [Informative] **Public Sector Profile of the Pan-Canadian Trust Framework Consolidate Overview Version 1.4** <https://github.com/canada-ca/PCTF-CCP/blob/master/Version1_4/PSP-PCTF-V-1.4-Consolidated-Overview-EN-2021-12-16.pdf>
3. [Informative] **Public Sector Profile of the Pan-Canadian Trust Framework Assessment Workbook** <https://github.com/canada-ca/PCTF-CCP/blob/master/Version1_4/PSP-PCTF-V1.4-Assessment-Workbook-2021-12-16.xlsx>
4. [Informative] **Treasury Board of Canada Directive on Identity Management** https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577

# Assessment Methodology

The scheme is designed to accommodate a broad range of scenarios. The normative core of the scheme consists of the following objects of conformity.

A trusted digital identity program can be made up of several components

## Objects of Conformity

### Conformity of Atomic Processes

1. **Enterprise-Wide Management:** General requirements for enterprise-wide management that are applicable to all processes identified in the PCTF
2. **Identity Domain General:** General requirements for the identity domain atomic processes
3. **Identity Domain Atomic Processes:** Specific requirements for the atomic processes that comprise the identity domain
4. **Credential Domain General:** General requirements for the credential domain atomic processes
5. **Credential Domain Atomic Processes:** Specific criteria for the atomic processes that comprise the credential domain
6. **Relationship Domain General:** General requirements for the relationship domain atomic processes
7. **Relationship Domain Atomic Processes:** Specific criteria for the atomic processes that comprise the relationship domain
8. **Consent Domain General:** General requirements for the consent domain atomic processes
9. **Consent Domain Atomic Processes:** Specific criteria for the atomic processes that comprise the consent domain
10. **Signature Domain General:** General requirements for the signature domain atomic processes
11. **Signature Domain Atomic Processes:** Specific criteria for the atomic processes that comprise the signature domain.

### Conformity of Subject Entities

1. Persons
2. Organizations
3. Relationships

### Conformity Assessment Qualifiers

1. Identity Assurance Levels for **Persons**
2. Identity Assurance Levels for **Organizations**
3. Credential Assurance **Levels**
4. Relationship **Assurance**

## Determining Scope of Assessment

# Marks

### Digital Representations

A Digital Representation is an electronic representation of an Entity or an electronic representation of an association between two or more Entities. Digital Representations are intended to model real-world Entities, such as persons and organizations. The scheme defines two types of **Digital Representations**:

* **Digital Identity:** An electronic representation of an Entity that is exclusive to the Entity. Currently the scheme defines, **Persons** and **Organizations**.
* **Digital Relationship:** An electronic representation of an association between two or more Entities.

Over time, as the scheme evolves, Digital Representations will be extended to include other types of Entities such as digital assets.

### Identity Types

Broadly, an identity is defined as a reference or designation used to uniquely distinguish a particular Entity within a population. There are two types of identity: foundational identity and contextual identity.

* A **Foundational Identity** is an identity that has been established or changed as a result of a foundational event (e.g., birth, person legal name change, immigration, legal residency, naturalized citizenship, death, organization legal name registration, organization legal name change, or bankruptcy).
* A **Contextual Identity** is an identity that is used for a specific purpose within a specific identity context9 (e.g., banking, business permits, health services, drivers licensing, or social media). Depending on the identity context, a contextual identity may be tied to a foundational identity (e.g., a drivers licence) or may not be tied to a foundational identity (e.g., a social media profile).

### Establishment and Maintenance of Identities

The establishment and maintenance of foundational identities are under the exclusive control of the public sector; specifically:

**For Persons**

* The Vital Statistics Organizations (VSOs) of the Provinces and Territories – responsible for the establishment and maintenance of the foundational identity of persons born in Canada
* Immigration, Refugees, and Citizenship Canada (IRCC) – responsible for the establishment and maintenance of the foundational identity of the following types of persons:
* Canadians born outside of Canada
* permanent residents in Canada
* temporary residents in Canada
* refugee claimants
* foreign-born visitors

**For Organizations**

* The Business Registries of the Provinces and Territories
* The Federal Corporate Registry of Corporations Canada

Contextual identities are established and maintained by both the public and private sectors.

### Trusted Digital Identity

Put standard stuff here

Programs that provide trusted digital identities (‘TDI’) are complex distributed programs that that have evolved from existing programs combined with new and evolving practices.

## Conformity Assessment Activities

Enagement stuff here

Overview of assessment methods here

### Initial Conformity Assessment

## Process Mapping

Process mapping consists of the set of activities to map program activities, business processes, and technical capabilities to the atomic processes defined in the scheme. In most cases, this mapping is applied to an existing program/service currently in operation, but it may also be used as an aid in the design of a new program/service. The table below gives some examples of mapping atomic processes to business processes.

Ongoing Assessment and Surveillance Activities

# Assessment Methodology

## Atomic and Compound Processes

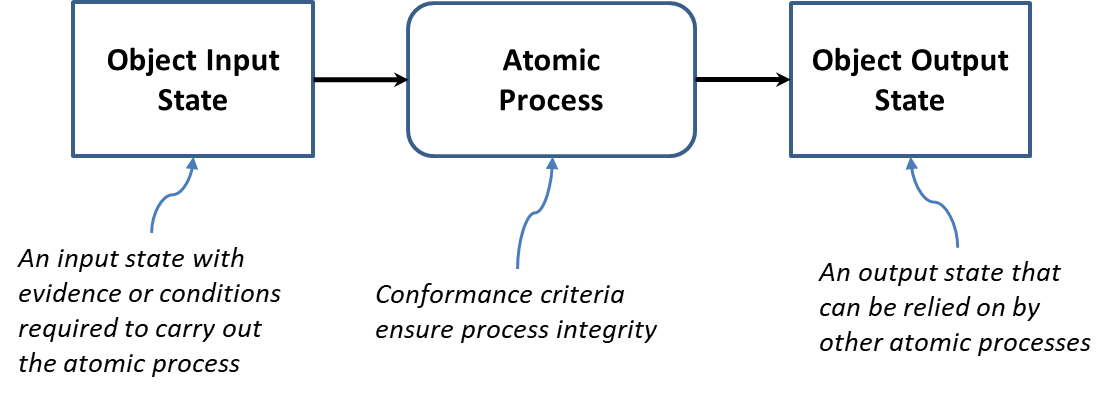
The scheme defines a set of atomic processes that can be separately assessed and certified to be compatible with one another in a digital ecosystem. An atomic process is a set of logically related activities that results in a state transition. The CAS recognizes that in practice a business process is often a collection of atomic processes that results in a set of state transitions. These collections of atomic processes are referred to as compound processes.

The atomic processes have been defined in a way that they can be implemented as modular services and be separately assessed for certification. Once an atomic process has been certified, it can be relied on or “trusted” and integrated into other digital ecosystem platforms. The digital ecosystem is intended to interoperate seamlessly across different organizations, sectors, and jurisdictions, and to be interoperable with other trust frameworks.

It should be noted that, while most atomic processes are employed many times by a program/service, four atomic processes – Identity Information Determination, Identity Evidence Determination,Relationship Information Determination, and Relationship Evidence Determination – are carried out only once for a program/service.

## Atomic Processes

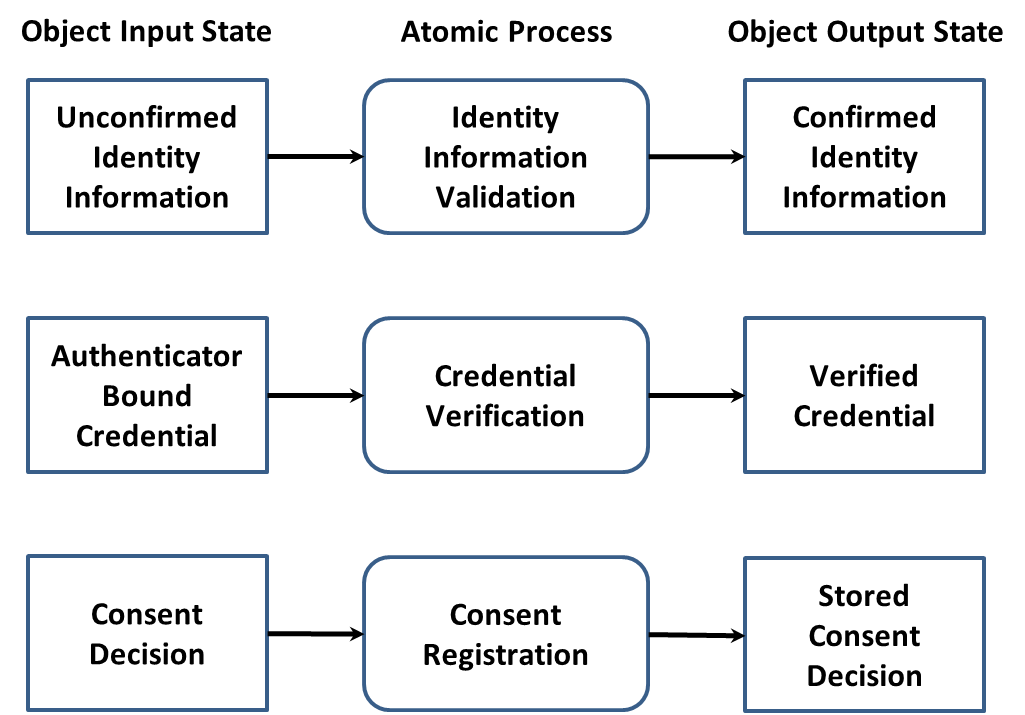
An atomic process is a set of logically related activities that results in the state transition of an object. The object’s output state can be relied on by other atomic processes. Figure 5 illustrates the atomic process model.



Atomic processes are crucial building blocks to ensuring the overall integrity of the Digital Identity supply chain and therefore, the integrity of digital services. The integrity of an atomic process is paramount because the output of an atomic process is relied upon by many participants – across jurisdictional and public and private sector boundaries, and over the short term and the long term. The PCTF ensures the integrity of an atomic process through a set of well-defined conformance criteria that support an impartial, transparent, and evidence-based assessment and certification process.

The conformance criteria associated with an atomic process specify what is required to transform an object’s input stateinto anoutput state. The conformance criteria ensure that the atomic process is carried out with integrity. For example, an atomic process may involve assigning an identifier to an Entity. The conformance criteria may specify that the party responsible for carrying out the atomic process must ensure that the identifier assigned to the Entity is unique for a specified population.

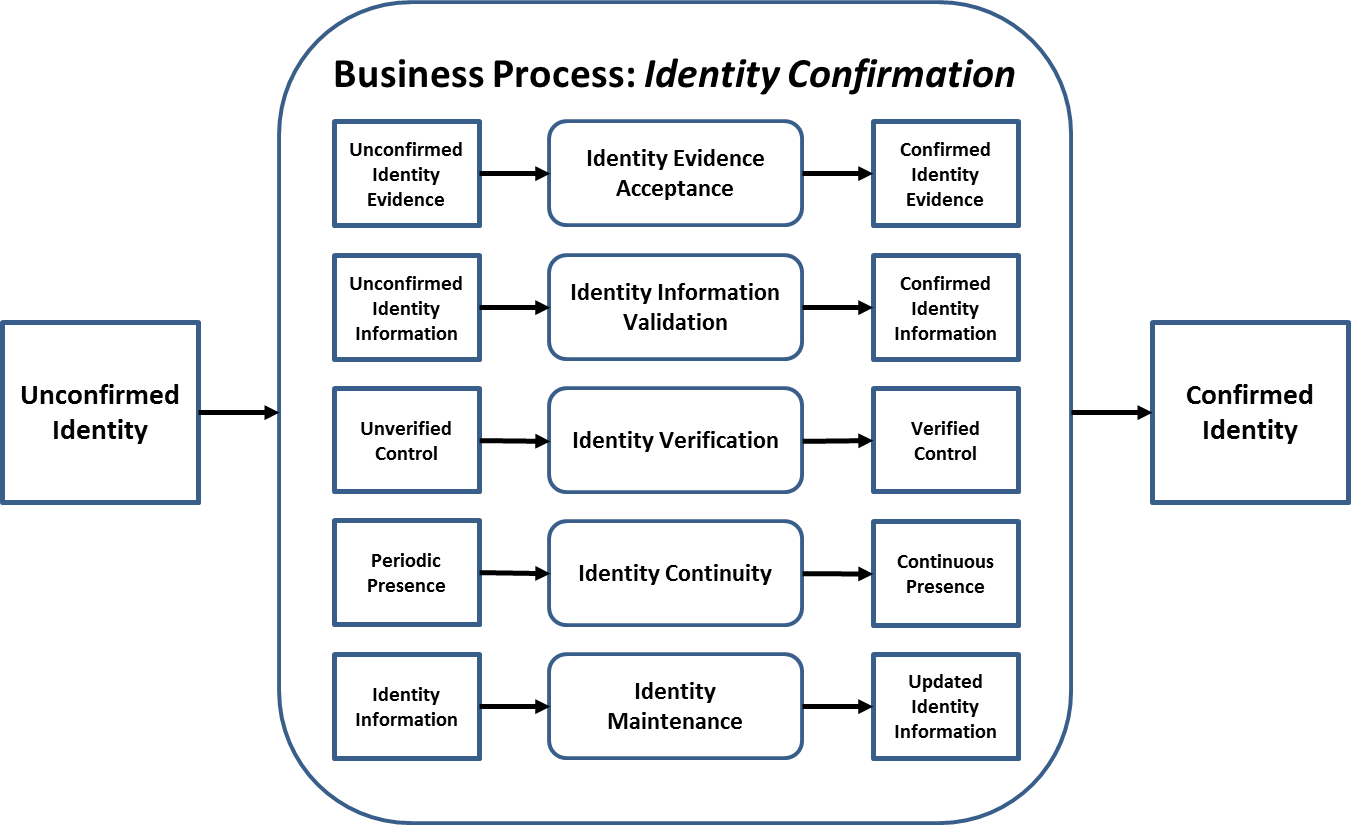
The figure below illustrates some model diagrams of three atomic processes.



### Compound Processes

The primary function of the CAF is to assess and certify business processes. When analyzed, business processes are often composed of several atomic processes. A set of atomic processes grouped together form a compound process that results in a set of state transitions. It may also be the case that a compound process is composed of a set of other compound processes which in turn can be decomposed into a set of atomic processes.

For example, a business process that one party refers to as *Identity Confirmation* may in fact turn out to be a compound process consisting of 5 atomic processes as shown in the following figure.



**Note**: Any ordering of the atomic processes should not be inferred from the diagram.

### Dependencies

The CAS recognizes two types of dependencies. The first type of dependency is a dependency that exists between two or more atomic processes. Although each atomic process is functionally discrete, to produce an acceptable output an atomic process may require the successful prior execution of another atomic process. For example, although Identity Establishment of an Entity can be performed independently at any time, it is logically correct to do so only after Identity Resolution for that Entity has been achieved. This type of dependency is specified in the conformance criteria.

The second type of dependency is a dependency on an external organization (e.g., a credential service provider) for the provision of one or more atomic process outputs. This type of dependency is identified and noted in the assessment process.

# Conformity Assessment Criteria

Conformance criteria are a set of requirement statements that define what is necessary to ensure the integrity of an atomic process. Conformance criteria are used to support an impartial, transparent, and evidence-based assessment and certification process.

For example, the Identity Resolution atomic process usually involves assigning an identifier to an Entity. The conformance criteria specify that the atomic process must ensure that the identifier that is assigned to the Entity is unique for a specified population.

The conformance criteria are maintained in a separate document – the *PSP PCTF Assessment Workbook*.

### Qualifiers

A qualifier and a value for the qualifier are associated with each conformance criterion. The qualifier value may indicate that the requirement is applicable for achieving a certain level of confidence or stringency; or that the requirement is to be applied to a specific identity type; or that it is a policy or regulatory requirement, or a requirement of another trust framework. Qualifiers are used to select the applicable conformance criteria to be used in the assessment process.

Qualifiers can also be used to map conformance criteria to jurisdictional policy or regulatory requirements. For example, the conformance criteria for the Identity Verification atomic process that have a Pan-Canadian Level of Assurance Qualifier value of “IP1” can be mapped to Identity Assurance Level 1 as defined in the *Standard on Identity and Credential Assurance* issued by the Treasury Board Secretariat of Canada. In addition, qualifiers can be used to facilitate the mapping of conformance criteria equivalencies across different trust frameworks.

A conformance criterion may have a single qualifier value (i.e., the conformance criterion is applicable in only a certain case), or several qualifier values (i.e., the conformance criterion is applicable in several cases). Consult the *PSP PCTF Assessment Workbook* (a separate document) for examples of how qualifiers and their values are used for assessment and how they may be mapped to other frameworks.

# Additional References

### 

### 