IDENTITY MANAGEMENT SUB-COMMITTEE (IMSC)

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

VERSION 1.1

Document Version:	0.2
Document Status:	Consultation Draft
Date:	2019-10-31
Security Classification:	UNCLASSIFIED

DOCUMENT VERSION CONTROL

Version Number	Date of Issue	Author(s)	Brief Description
0.1	2019-10-10	IMSC PCTF WG	Consultation Draft
0.2	2019-10-31	IMSC PCTF WG	Consultation Draft

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

This document describes **Version 1.1** of the public sector profile of the ***Pan-Canadian Trust Framework (PCTF)***. The document is structured as follows:

- **Sections 1 through 3** provide the purpose of the document, and a description of the context, stakeholder community, and goals of the PCTF
- **Section 4** provides the key concepts and elements of the PCTF
- **Sections 5 through 9** provide various appendices that cover terms and definitions, discussions on selected topics related to the PCTF, and a bibliography

The Pan-Canadian Trust Framework is designed to enable the transition to a digital identity ecosystem. Digital identity offers a transformative solution to service delivery for Canadians. Digital identity can increase efficiency and enable innovative ways of conducting existing business processes such as open banking, business licencing, and government service delivery.

The PCTF is simple and integrative; technology-agnostic; complementary to existing frameworks; clearly linked to policy, regulation, and legislation; and is designed to apply relevant standards to key processes and capabilities. The PCTF facilitates a common approach between all levels of government and the private sector thereby serving the needs of different communities who need to trust digital identities. The PCTF is defined in a way that encourages innovation and the evolution of the digital identity ecosystem. The PCTF allows for the interoperability of different platforms, services, architectures, and technologies working together as a coherent whole.

The PCTF defines two types of ***digital representations*** required for the digital identity ecosystem: 1) ***digital identities*** of persons and organizations, and 2) ***digital relationships*** between persons, between organizations, and between persons and organizations.

The PCTF supports the acceptance of digital identities and digital relationships by defining a set of atomic processes that can be mapped to existing business processes, independently assessed using conformance criteria, and certified to be trusted and interoperable within the many contexts that comprise the digital identity ecosystem.

1 PURPOSE OF THIS DOCUMENT

The purpose of this document is to describe the public sector profile of the Pan-Canadian Trust Framework (PCTF)[1].

The audience for this document includes:

- members of the digital identity community from the public and private sectors (including regulatory and standards bodies) – as key stakeholders and contributors to the PCTF;
- digital identity technology and service providers – to understand where they fit in the PCTF, to help define requirements for their products and services, and to assess the integrity of their processes; and
- digital identity consumers and program/service providers – to assess the value of employing digital identity solutions and processes when interacting online.

2 TERMS AND DEFINITIONS

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

[1] Development of the public sector profile of the Pan-Canadian Trust Framework is a collaborative effort led by the Identity Management Sub-Committee (IMSC) of the Joint Councils of Canada, a forum consisting of the Public Sector Chief Information Officer Council (PSCIOC) and the Public Sector Service Delivery Council (PSSDC). This document has been developed by the IMSC PCTF Working Group (IMSC PCTF WG) for the purposes of discussion and consultation, and its contents have not yet been endorsed by the IMSC or the Joint Councils. This material is published under the *Open Government License – Canada* which can be found at: https://open.canada.ca/en/open-government-licence-canada.

3 CONTEXT, STAKEHOLDER COMMUNITY, AND GOALS

3.1 Context

In the domain of identity management there are two primary identity models: the centralized model and the federated model. Both models recognize the need for clearly defined functional roles such as authoritative source, identity provider, credential provider, authentication provider, and relying party.

Canada, as a federal polity has multiple jurisdictions with diverse mandates and needs. This results in an ecosystem of multiple identity providers relying on authoritative source registries that span provincial and federal jurisdictions. As a consequence, a Canadian digital identity ecosystem requires a federated identity model.

A federated identity model allows for cooperation between multiple jurisdictions that have agreed to work together. A federation enables interoperability of standards by creating mutual agreements across the public and private sector through service agreements, legal obligations, and dispute resolution mechanisms. These components are referred to as federated trust frameworks.

The verifiable credentials model is the newest identity model to emerge. This model disrupts the need for trusted third parties for certain types of transactions such as authentication and identity proofing. Because the verifiable credentials model is still in its infancy, it is anticipated that the traditional models will co-exist with the newer model for the foreseeable future.

3.2 Stakeholder Community

A shared vision across stakeholders, aligned through goals will help foster a digital identity ecosystem. The stakeholder community of the PCTF consists of:

- **Individuals**: Individuals who require proof of identity to access programs and services are one set of end users of the digital identity ecosystem. Individuals have the right to exercise appropriate control over how their data is collected, used, stored, and shared.

- **Federal Government**: Federal government departments and agencies provide services and benefits to individuals and organizations. As relying parties, they trust digital identity providers as authoritative sources of identity. The federal government can also be an authoritative source of identity (i.e., Corporations Canada and Immigration, Refugees, and Citizenship Canada).

- **Provincial and Territorial Governments**: Provincial and territorial governments as authoritative sources of identity are digital identity providers. Provincial and territorial governments conduct identity proofing by means of their vital statistics registries, business registries, health registries, and drivers licencing registries.

- **Private Sector**: Private sector companies are end users of government services such as licencing and tax rebates. The private sector relies on government authoritative parties for identity proofing. Private sector companies as developers and innovators are also suppliers of digital identity solutions.

3.3 Goals

It is proposed that the PCTF be guided by the goals published by the World Bank[2]:

Inclusivity: Digital identity requires a network of interconnected systems across federal-provincial lines that enable a digital identity to be inclusive of all needs. Digital inclusivity should strive for continuous identity from birth to death and be accessible by all residents of Canada. By enabling digital inclusivity from the start, the PCTF aims to mitigate the digital divide that leads to the unequal distribution of benefits.

Robustness: The Pan-Canadian Trust Framework enables a robust digital identity by championing interoperability. By encouraging risk sharing between authoritative and relying parties, the PCTF enables governments to think beyond processes and solutions that are locked in by vendors. Technical interoperability is founded on open source and international standards and regulations. By opting for interoperability, the PCTF creates a level playing field that is not captured by a single provider or technology. In this way, the PCTF enables market interoperability by allowing for competition among digital identity solutions and innovations.

Trust: To ensure that the rights of citizens are protected, a robust digital identity must also be a trusted digital identity. The digital Identity ecosystem must be built on legal and operational foundations of trust and accountability between the federal and provincial/territorial governments, the private sector, and individuals. People must be assured of the protection of their data through the ability to exercise and control its use. Trust translates into establishing clear institutional mandates and accountability. Ecosystem-wide governance arrangements for identification should specify institutional relations among parties, so that the rights and responsibilities are clear. This trusted infrastructure allows for transparency of roles and responsibilities of identity providers. Furthermore, user rights means that identity providers should be transparent in identity management by developing mechanisms that promote data minimization.

[2] For more information, see *ID4D Practitioner's Guide [WB, 2019].*

4 THE PAN-CANADIAN TRUST FRAMEWORK

4.1 Overview of the PCTF

The Pan-Canadian Trust Framework is one outcome of the Pan-Canadian approach for identity management[3] (PCIM). PCIM is an agreement of principles and standards to develop solutions for use by all Canadians.[4] This approach recognizes that while there are dependencies and differences between organizations, a seamless and citizen-centric approach to digital service delivery can be achieved by defining an agreed upon methodology that is implemented and assessed in a consistent manner.

The Pan-Canadian Trust Framework has the following characteristics:

1. **A simple and integrative framework** that is easy to understand yet capable of being applied in a complex environment
2. **Technology-agnostic**: provides flexibility and logical precision in assessing the trustworthiness of digital identity solutions and digital identity providers
3. **Complements existing frameworks** (security, privacy, service delivery, etc.)
4. **Provides clear links to applicable policy, regulation, and legislation** through defined conformance criteria
5. **Normalizes (standardizes) key processes and capabilities** to enable cross-sector collaboration and digital identity ecosystem development

It should be noted that the PCTF, in itself, is not a governance framework. Rather, it is a tool to help put into effect relevant legislation, policy, regulation, and agreements between parties.

[3] For a general introduction to identity management concepts see *Appendix B: Identity Management Overview*.

[4] Available at (public sector registration required): https://gccollab.ca/file/view/36223/imsc-paper-trusting-identities-consultation-draft-enpdf.

4.2 Key Concepts

4.2.1 Scope of the PCTF

The scope of the PCTF is:

- the universe of persons in Canada which is defined as all living persons resident in or visiting Canada, as well as all deceased persons, for whom an identity has been established in Canada;
- the universe of organizations in Canada which is defined as all organizations registered and operating in Canada, as well as inactive organizations, for which an identity has been established in Canada; and
- the universe of relationships in Canada of persons to persons, organizations to organizations, and persons to organizations.

4.2.2 The PCTF Model

The PCTF model consists of a set of PCTF processes enabled by a supporting infrastructure to create digital representations. This is illustrated in Figure 1.

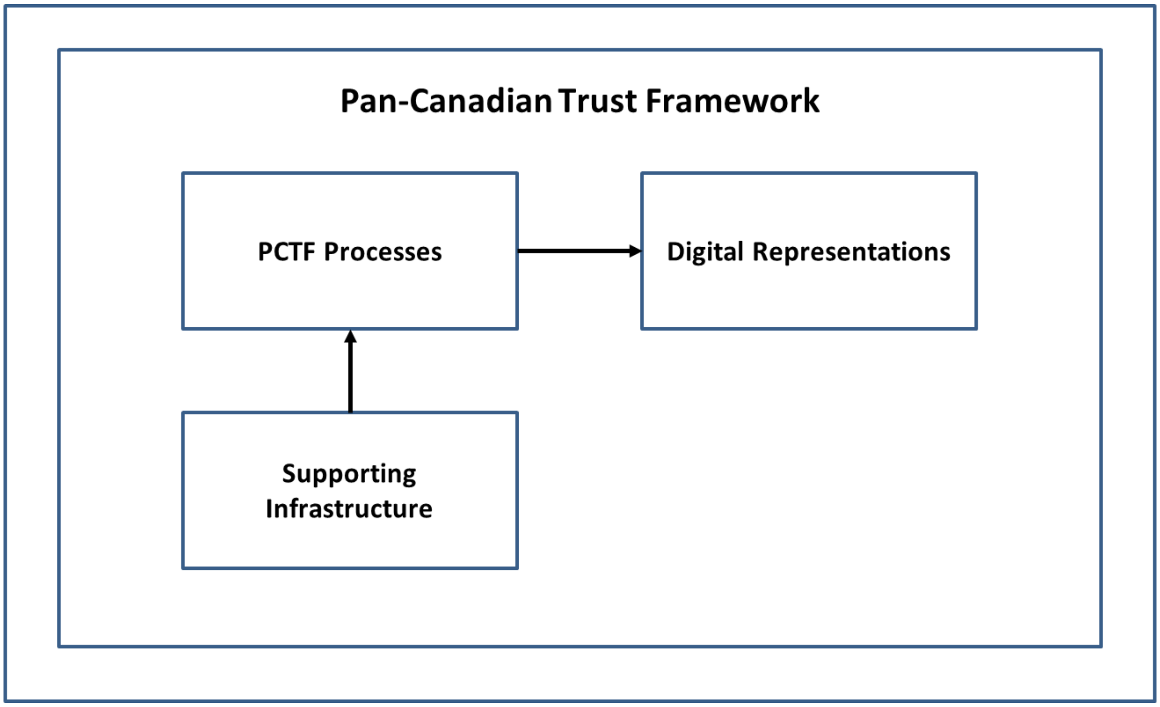


Figure 1: The PCTF Model

4.2.3 PCTF Processes

The PCTF defines a set of atomic processes that can be independently assessed and certified to interoperate with one another in a digital identity ecosystem. An atomic process is a set of logically related activities that results in a state transition. The PCTF also defines a set of compound processes. A compound process is a collection of atomic processes, and/or other compound processes that results in a set of state transitions. All of the atomic processes have been defined in a way that they can be implemented as modular services and be independently assessed for certification. Additional atomic processes can be added as required and all of the atomic processes can be mapped to various conformance criteria qualifiers.

Once an atomic process has been certified, it can be relied on or “trusted” and integrated into other digital identity ecosystem platforms. This digital identity ecosystem is intended to interoperate seamlessly across different organizations, sectors, and jurisdictions, and to be interoperable with other trust frameworks.

4.2.4 Digital Representations

A digital representation is an electronic representation of any entity that can be subject to legislation, policy, or regulations within a context and which may have certain rights, duties, and obligations; or an electronic representation of the relationship between such entities. Digital representations are intended to model real-world actors, such as persons and organizations.

Currently, the PCTF recognizes two types of digital representations:

1. **Digital Identity**: A digital identity is an electronic representation of a person or organization, used exclusively by that same person or organization, to access valued services and to carry out transactions with trust and confidence.
2. **Digital Relationship**: A digital relationship is an electronic representation of the relationship of one person to another person, one organization to another organization, or a person to an organization.

As the PCTF evolves these digital representations may be extended to include other entity types such as assets and contracts (i.e., digital assets and smart contracts).

4.2.5 Supporting Infrastructure

The Supporting Infrastructure is the set of technical, operational, and policy enablers that serve as the underlying infrastructure of the PCTF. While these enablers are crucial to the PCTF, they are situated in the Supporting Infrastructure because they already have established tools and processes associated with them (e.g., Privacy Impact Assessment, Security Assessment and Authorization). The goal of the PCTF is to leverage as many of these tools and processes as possible, while maintaining a focused set of PCTF-specific atomic processes and conformance criteria.

Figure 2 illustrates the current iteration of the Supporting Infrastructure. In this iteration, many of the boxes are placeholders to indicate further investigation or future development.

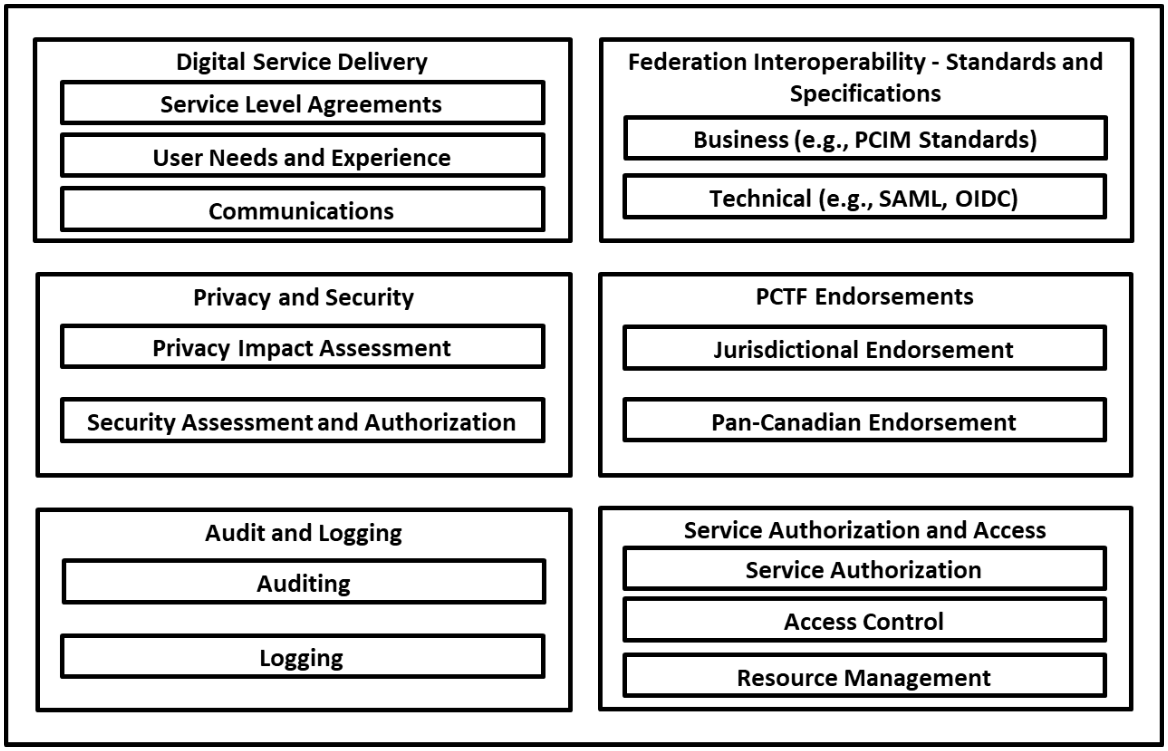

Digital Service Delivery
Service Level Agreements
User Needs and Experience
Communications
Federation Interoperability - Standards and Specifications
Business (e.g., PCIM Standards)
Technical (e.g., SAML, OIDC)
Privacy and Security
Privacy Impact Assessment
Security Assessment and Authorization
PCTF Endorsements
Jurisdictional Endorsement
Pan-Canadian Endorsement
Audit and Logging
Auditing
Logging
Service Authorization and Access
Service Authorization
Access Control
Resource Management

Figure 2: Supporting Infrastructure

4.2.6 Identity Domains

The PCTF draws a clear distinction between *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, citizenship, death, organization legal name registration, organization legal name change, bankruptcy). A contextual Identity is an identity that is used for a specific purpose within a specific identity context[5]. A contextual identity may or may not be tied to a foundational identity. The establishment and maintenance of foundational identities is the exclusive domain of the public sector (more precisely, the Vital Statistics Organizations (VSOs) and Business Registrars of the Provinces and Territories, Immigration, Refugees, and Citizenship Canada (IRCC), and the Federal Corporate Registrar). Contextual identities are the domain of both the public and private sectors. Figure 3 shows the identity domains.

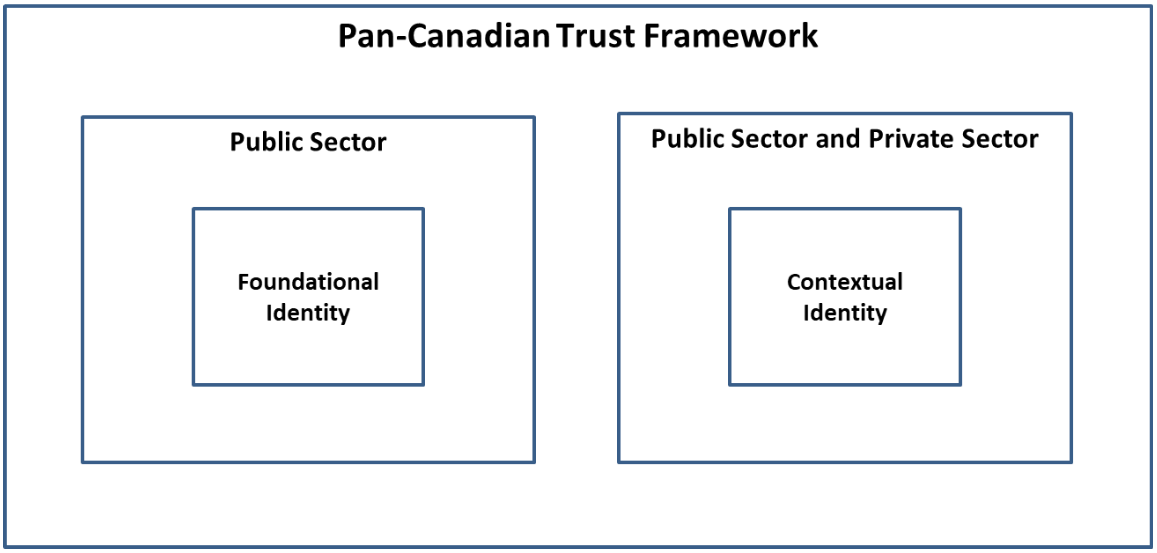

Pan-Canadian Trust Framework
Public Sector
Foundational Identity
Public Sector and Private Sector
Contextual Identity

Figure 3: Identity Domains

[5] In delivering their programs and services, program/service providers operate within a certain environment or set of circumstances, which in the domain of identity management is referred to as the identity context. Identity context is determined by factors such as mandate, target population (i.e. clients, customer base), and other responsibilities prescribed by legislation or agreements. For more information on identity and identity management concepts, see Appendix B.

4.3 Overview of PCTF Processes

4.3.1 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 as a *proof* by other processes. Figure 4 illustrates the *atomic process model*.

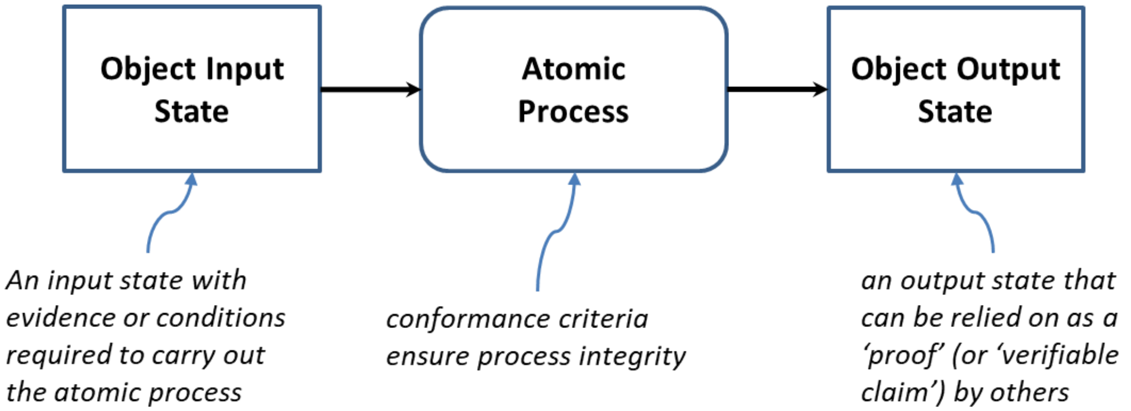

Object Input State
Atomic Process
Object Output State
An input state with evidence or conditions required to carry out the atomic process
conformance criteria ensure process integrity
an output state that can be relied on as a 'proof' (or 'verifiable claim') by others

Figure 4: 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 agreed upon and 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 state into an output 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 a person or organization. The conformance criteria may specify that any entity responsible for carrying out the atomic process must ensure that the identifier assigned to the person or organization is unique for a certain population.

Currently, the PCTF recognizes 24 atomic processes:

- Identity Resolution
- Identity Establishment
- Identity Validation
- Identity Verification
- Evidence Validation
- Identity Presentation
- Identity Maintenance
- Identity-Credential Binding
- Identity Linking
- Credential Issuance
- Credential-Authenticator Binding
- Credential Suspension
- Credential Recovery
- Credential Revocation
- Credential Authentication
- Create Signature
- Check Signature
- Formulate Notice
- Request Consent
- Record Consent
- Review Consent
- Renew Consent
- Expire Consent
- Revoke Consent

These atomic processes are detailed in Section 4.4.

Figure 5 illustrates some model diagrams of three atomic processes.

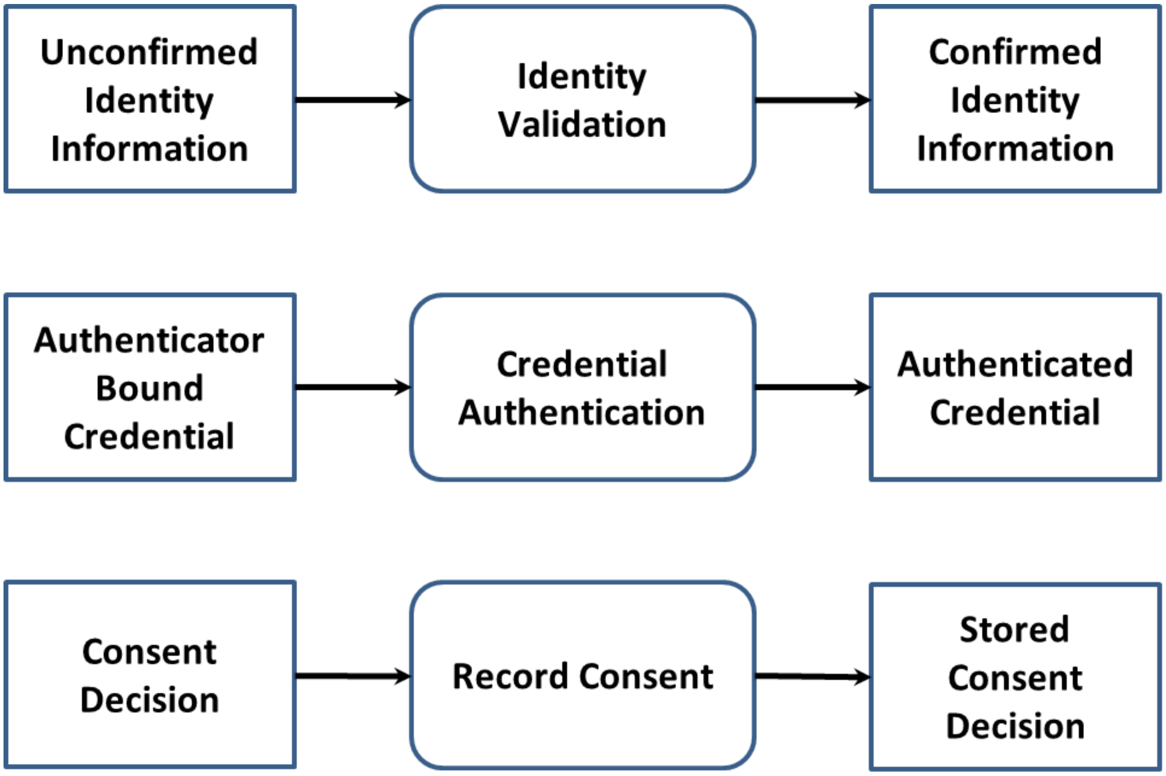

Unconfirmed Identity Information
Identity Validation
Confirmed Identity Information
Authenticator Bound Credential
Credential Authentication
Authenticated Credential
Consent Decision
Record Consent
Stored Consent Decision

Figure 5: Examples of Atomic Processes (Modeled)

4.3.2 Compound Processes

In most instances the PCTF will be used to assess existing business processes. When analyzed, these business processes are often composed of several atomic processes. The PCTF allows a set of atomic processes to be grouped together to form a *compound process* that results in a set of state transitions. The output of a compound process can be viewed as a set of proofs. 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.

Three compound processes – ***Identity Assurance***, ***Credential Assurance***, and ***Informed Consent*** – constituted the original conception of the digital identity of a person, and have been used to develop policy requirements; these three compound processes are detailed in Section 4.5.

Other compound processes that have been identified include:

- Identity Creation
- Identity Confirmation
- Credential Creation
- Credential Confirmation
- Identity Registration
- Service Registration
- Digital Identity Creation
- Service Enrolment

For example, *Identity Confirmation* is a compound process consisting of 5 atomic processes as shown in Figure 6 (Note: any ordering of the atomic processes should not be inferred from the diagram).

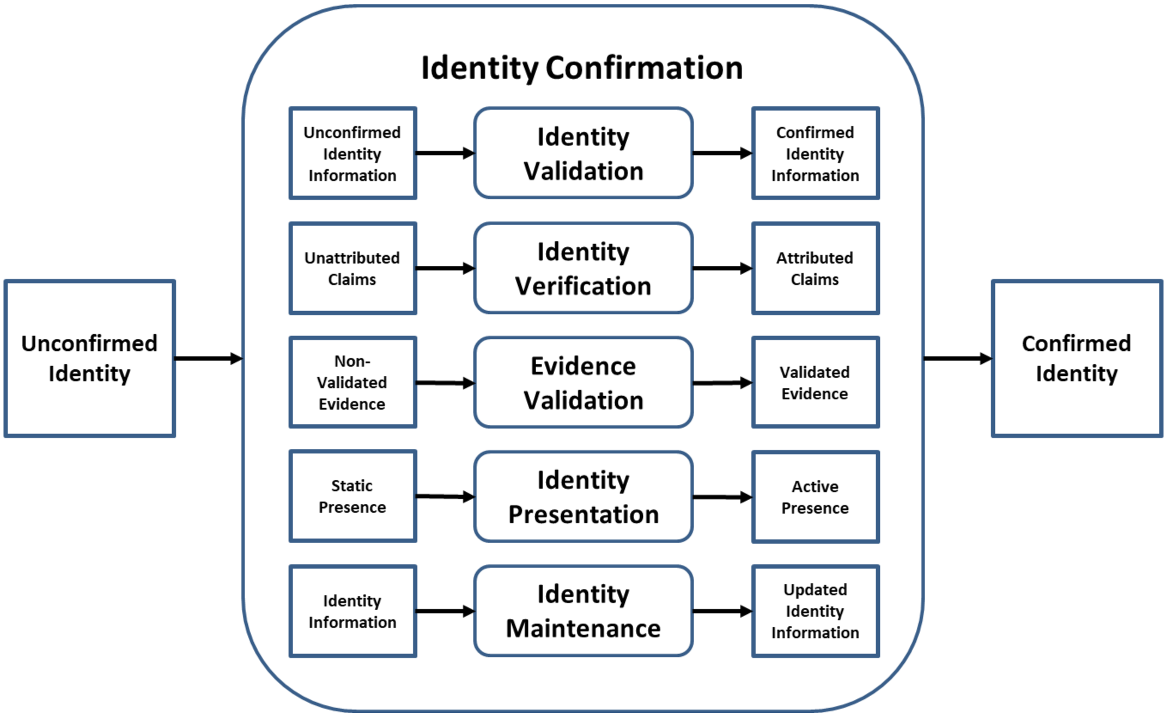


Figure 6: Identity Confirmation Compound Process

4.3.3 Dependencies

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. This is referred to as a dependency. For example, although *Identity Establishment* of a person or organization can be performed independently at any time, it is logically correct to do so only after *Identity Resolution* for that person or organization has been achieved.

4.3.4 Mapping Atomic Processes to Existing Business Processes

An existing business or technical process may be designated as an atomic process that is subject to the conformance criteria, assessment process, and certification defined by the PCTF. In addition, existing programs or services often have embedded identity-related compound processes (e.g., “identity proofing”, “identity registration”) that consist of several atomic processes.

Processes that were originally developed to work within a particular context may be leveraged and relied on as atomic processes within the Pan-Canadian Trust Framework. This is done by mapping the existing processes into the atomic process definitions. Once mapped, these processes can be assessed and certified using the defined conformance criteria associated with the corresponding atomic processes.

The following table lists some example mappings of atomic processes to existing business processes:

Atomic Process	Existing Business Process Examples
Identity Resolution	A vital statistics registration process that collects uniquely identifying biographical or ‘tombstone’ data (name, date of birth) associated with a person A business registrar process that collects uniquely identifying data (legal name) associated with an organization
Identity Establishment	A birth registration process that creates an authoritative birth record A program enrolment process that creates a user account profile A business registrar process that create an authoritative business record
Identity Validation	A driver’s license application process that confirms information as presented on physical documents or by means of an electronic validation service

Atomic Process	Existing Business Process Examples
	A cannabis licensing process that confirms information as presented about a business by means of an electronic validation with the applicable business registrar
Identity Verification	A passport application process that compares biometric traits recorded on a document (e.g., facial photograph, eye colour, height, etc.) to ensure it is the right applicant Asking a presenting person questions that only they would know (e.g., credit history question, shared secrets, mailed-out access codes, etc.) A financial tracking process that confirms that the organization performs its listed services and that the owner appears in the applicable registrar and that they are eligible to own or direct the service that an organization offers
Identity Maintenance	Message-based (push) notification update services Regularly-scheduled (pull) validation services Mandatory updates based on dates of expiry or enforced validity periods
Credential Issuance	Issuing an authoritative document such as a birth certificate or driver's licence Issuing an authoritative document such as a certificate of existence or compliance Issuing a verifiable digital credential

The mapping exercise may need to span several providers. It may be the case that a single provider does not carry out all of the atomic processes related to a compound process – some of the atomic processes might be carried out by other providers. It may also be the case that the atomic processes are repeated in another context. For example, a relying party, in consuming a digital identity from a provider, may carry out the identity resolution atomic process within their own context to ensure that they are dealing with the right person or organization. In addition, the PCTF may be used by a relying party to map their own existing processes when consuming a digital identity from a provider.

4.3.5 Proofs and Conveyance

The PCTF has been defined to be enabled by different platforms and architectures, all of which may co-exist with one another in the digital identity ecosystem. For example, established federated identity platforms and solutions using Secure Assertion Markup Language (SAML) and Open ID Connect (OIDC) protocols may co-exist with emerging decentralized claim-based approaches using digital wallets. The PCTF does not constrain the possibility of several competing providers and it is anticipated that many providers will coexist to serve the needs of different communities across the public and private sector.

To facilitate the co-existence of these different providers and different solution approaches, the PCTF distinguishes between the proofs (i.e., the inputs and outputs) that are consumed and produced by PCTF processes, and the conveyance of the proofs (i.e., how a proof is carried across a network and made available to another party).

Proofs are independent of the conveyance model. The proofs can be conveyed between parties using a traditional/centralized model (e.g., a trusted third party) or a decentralized model (e.g., a distributed ledger) – or both. The proofs can also be passed directly between parties. As can be seen in Figure 7, the conveyance model exists in between the parties producing and consuming the proofs.

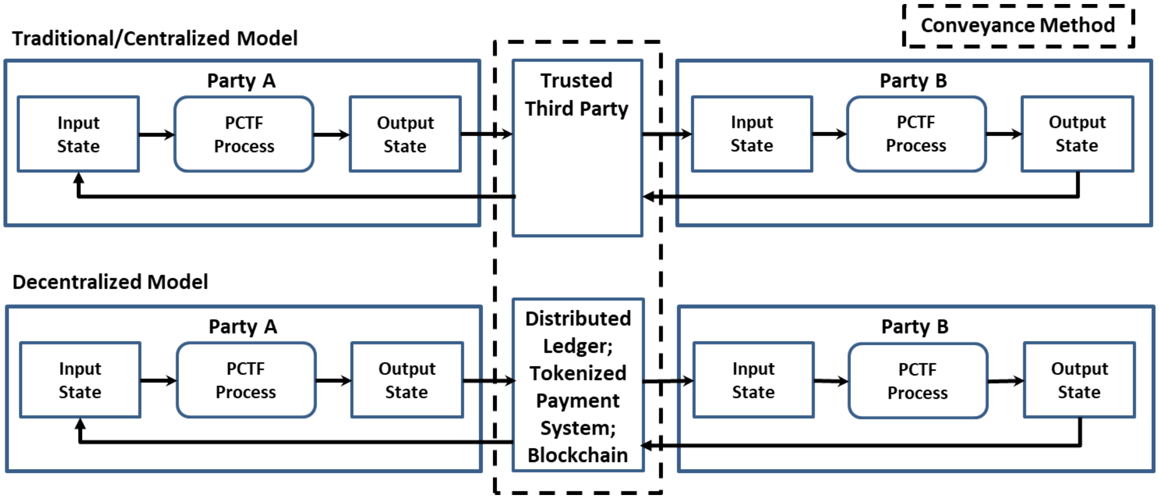


Figure 7: Conveying Proofs between Parties

Requirements specific to conveyance methods are considered to be part of the Supporting Infrastructure, and will be developed as part of technical interoperability requirements, standards, and specifications.

4.4 Atomic Processes in Detail

4.4.1 Identity Resolution

Process Description	Identity Resolution is the process of establishing the uniqueness of a person or organization within a program/service population through the use of identity information. A program or service defines its identity resolution requirements in terms of identity attributes; that is, it specifies the set of identity attributes that is required to achieve identity resolution within its population.
Input State	**Non-Unique Identity Information**: The identity information is not unique to one and only one person or organization
Output State	**Unique Identity Information**: The identity information is unique to one and only one person or organization

4.4.2 Identity Establishment

Process Description	Identity Establishment is the process of creating an authoritative record of identity within a program/service population that may be relied on by others for subsequent programs, services, and activities.
Input State	**No Authoritative Record**: No authoritative record exists
Output State	**Authoritative Record**: An authoritative record exists

4.4.3 Identity Validation

Process Description	Identity Validation is the process of confirming the accuracy of identity information about a person or organization as established by an authoritative party.
Input State	**Unconfirmed Identity Information**: The identity information has not been confirmed using an authoritative record
Output State	**Confirmed Identity Information**: The identity information has been confirmed using an authoritative record

4.4.4 Identity Verification

Process Description	Identity Verification is the process of confirming that the identity information being presented relates to the person or organization that is making the claim. It should be noted that this process may use personal information or organizational information that is not related to identity.
Input State	**Unattributed Claims**: The identity information has not been verified as being claimed by the rightful owner/user of the identity information
Output State	**Attributed Claims**: The identity information has been verified as being claimed by the rightful owner/user of the identity information

4.4.5 Evidence Validation

Process Description	Evidence Validation is the process of confirming that the evidence presented (whether physical or electronic) can be accepted or be admissible as a proof (i.e., beyond a reasonable doubt, balance of probabilities, and substantial likelihood).
Input State	**Non-Validated Evidence**: The object has not been confirmed as being an admissible proof
Output State	**Validated Evidence**: The object has been confirmed as being an admissible proof

4.4.6 Identity Presentation

Process Description	Identity Presentation is the process of dynamically confirming that a person or organization has a continuous existence over time (i.e., "genuine presence"). This process can be used to ensure that there is no malicious or fraudulent activity (past or present) and to address identity spoofing concerns.
Input State	**Static Presence**: The identity exists sporadically and often only in association with a vital event or business event (e.g., birth, death, bankruptcy)
Output State	**Active Presence**: The identity exists continuously over time in association with many transactions

4.4.7 Identity Maintenance

Process Description	Identity Maintenance is the process of ensuring that identity information is as accurate, complete, and up-to-date as is required.
Input State	**Identity Information**: The identity information is not up-to-date
Output State	**Updated Identity Information**: The identity information is more up-to-date

4.4.8 Identity-Credential Binding

Process Description	Identity-Credential Binding is the process of associating an identity with an issued credential.
Input State	**Issued Credential**: A unique credential has been assigned to the subject
Output State	**Identity Bound Credential**: An issued credential has been associated with an attributed actor

4.4.9 Identity Linking

Process Description	Identity Linking is the process of mapping two or more identifiers to the same identity for the purpose of facilitating identity resolution.
Input State	**Unlinked Identifier**: The identifier is not associated with another identifier
Output State	**Linked Identifier**: The identifier is associated with one or more other identifiers

4.4.10 Credential Issuance

Process Description	Credential Issuance is the process of creating and assigning a unique credential to a subject (i.e., a person, organization, or device). A credential includes one or more identifiers which may be pseudonymous, and may contain attributes verified by the credential issuer.
Input State	**No Credential**: No credential exists for the subject
Output State	**Issued Credential**: A unique credential has been assigned to the subject

4.4.11 Credential-Authenticator Binding

Process Description	Credential-Authenticator Binding is the process of associating an issued credential with one or more authenticators. This process also includes life-cycle activities such as removing authenticators, binding new authenticators, and updating authenticators (e.g., changing a password, updating security questions and answers, having a new photo taken).
Input State	**Issued Credential**: A unique credential has been assigned to the subject
Output State	**Authenticator Bound Credential**: An issued credential has been associated with one or more authenticators

4.4.12 Credential Suspension

Process Description	Credential Suspension is the process of transforming an issued credential into a suspended credential by flagging the issued credential as temporarily unusable.
Input State	**Issued Credential**: A unique credential has been assigned to the subject
Output State	**Suspended Credential**: The subject is not able to use the credential

4.4.13 Credential Recovery

Process Description	Credential Recovery is the process of transforming a suspended credential back to a usable state (i.e., an issued credential).
Input State	**Suspended Credential**: The subject is not able to use the credential
Output State	**Issued Credential**: A unique credential has been assigned to the subject

4.4.14 Credential Revocation

Process Description	Credential Revocation is the process of ensuring that an issued credential is permanently flagged as unusable.
Input State	**Issued Credential**: A unique credential has been assigned to the subject
Output State	**Revoked Credential**: The subject is not able to use the credential

4.4.15 Credential Authentication

Process Description	Credential Authentication is the process of verifying by means of an authenticator that a subject has control over their issued credential and that the issued credential is valid (i.e., not suspended or revoked).
Input State	**Authenticator Bound Credential**: An issued credential has been associated with one or more authenticators
Output State	**Authenticated Credential**: The subject has proven control of the issued credential and that the issued credential is valid

4.4.16 Create Signature

Process Description	Create Signature is the process of creating an electronic representation where, at a minimum: the person signing the data can be associated with the electronic representation; it is clear that the person intended to sign; the reason or purpose for signing is conveyed; and the data integrity of the signed transaction is maintained, including the original.
Input State	**No Signature**: No signature exists
Output State	**Signature**: A signature exists

4.4.17 Check Signature

Process Description	Check Signature is the process of confirming that the signature for the data is valid.
Input State	**Signature**: A signature exists
Output State	**Checked Signature**: The signature is valid

4.4.18 Formulate Notice

Process Description	Formulate Notice is the process of producing a notice statement that describes what personal information is being, or may be, collected; with which parties the personal information is being shared and what type of personal information is being shared; for what purposes the personal information is being collected, used, or disclosed; the risk of harm and other consequences as a result of the collection, use, or disclosure; how the personal information will be handled and protected; the time period for which the notice statement is applicable; and under whose jurisdiction or authority the notice statement is issued.
Input State	**No Notice Statement**: No notice statement exists
Output State	**Notice Statement**: A notice statement exists

4.4.19 Request Consent

Process Description	Request Consent is the process of presenting a notice statement to the subject (i.e., the natural person to whom the personal information in question pertains)[6] and asking the subject to agree to provide consent ("Yes") or decline to provide consent ("No") based on the contents of the notice statement, resulting in either a "yes" or "no" consent decision.
Input State	**Notice Statement**: A notice statement exists
Output State	**Consent Decision**: A consent decision exists

[6] The Request Consent atomic process assumes that the person providing consent has been the subject of both the Identity Assurance and Credential Assurance compound processes, and that consequently the person who is being asked to provide consent has the authority to do so.

4.4.20 Record Consent

Process Description	Record Consent is the process of persisting a notice statement and the subject's related consent decision, to storage. In addition, information about the subject, the version of the notice statement that was presented, the date and time that the notice statement was presented, and, if applicable, the expiration date for the consent decision may be stored. Once the consent information has been stored, a notification on the consent decision made is issued to the relevant parties to the consent decision.
Input State	**Consent Decision**: A consent decision exists
Output State	**Stored Consent Decision**: A stored consent decision exists

4.4.21 Review Consent

Process Description	Review Consent is the process of making the details of a stored consent decision visible to the subject or to an authorized reviewer.
Input State	**Stored Consent Decision**: A stored consent decision exists
Output State	**Stored Consent Decision**: A stored consent decision exists

4.4.22 Renew Consent

Process Description	Renew Consent is the process of extending the validity of a "yes" consent decision by means of increasing an expiration date limit.
Input State	**Stored Consent Decision**: A stored consent decision exists
Output State	**Stored Consent Decision**: A stored consent decision exists

4.4.23 Expire Consent

Process Description	Expire Consent is the process of suspending the validity of a "yes" consent decision as a result of exceeding an expiration date limit.
Input State	**Stored Consent Decision**: A stored consent decision exists
Output State	**Stored Consent Decision**: A stored consent decision exists

4.4.24 Revoke Consent

Process Description	Revoke Consent is the process of suspending the validity of a “yes” consent decision as a result of an explicit withdrawal of consent by the subject (i.e., a “yes” consent decision is converted into a “no” consent decision).
Input State	**Stored Consent Decision**: A stored consent decision exists
Output State	**Stored Consent Decision**: A stored consent decision exists

4.5 Compound Processes in Detail

4.5.1 Identity Assurance

The Identity Assurance compound process establishes a measure of certainty (or level of assurance) that a person, organization, or device is who or what they claim to be. This process is used to answer the question, "How sure are you that you have the right individual, organization, or device?” The Identity Assurance compound process consists of nine atomic processes. For each atomic process (described in detail in Section 4.4) there is a corresponding **input state**, **output state**, and **conformance criteria** used to standardize the atomic process and assess its integrity. The conformance criteria may also be profiled against **qualifiers** which indicate a requirement that can be traced to a level of assurance, an identity domain requirement, another trust framework requirement, or an applicable business, legal, policy, or regulatory requirement. Figure 8 illustrates the Identity Assurance compound process.

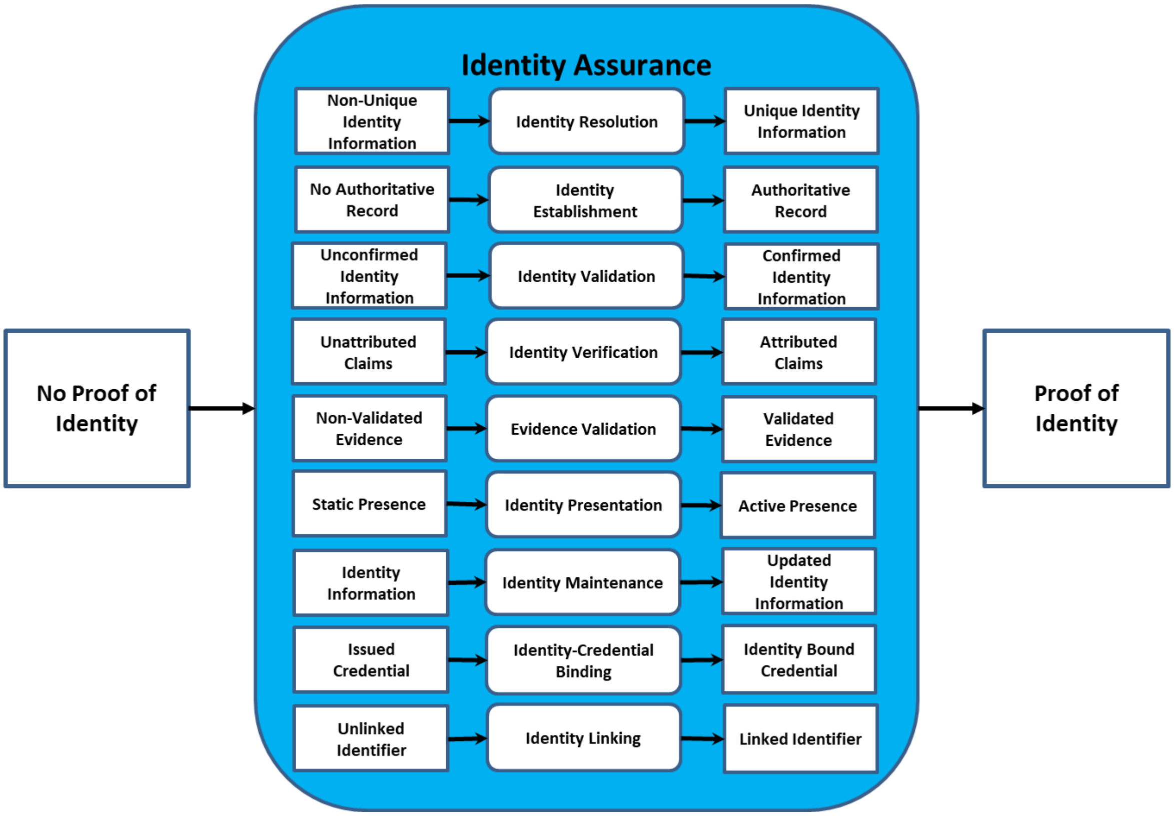


Figure 8: Identity Assurance Compound Process

A single provider may not be responsible for carrying out all the Identity Assurance atomic processes. It may be the case that the atomic processes are carried out by several different providers. For example, *Identity Validation* may be the responsibility of a vital statistics registrar, while *Identity Verification* may be the responsibility of the program/service provider. The involvement of several providers may introduce complexity in the assessment and certification process, and the PCTF enables or supports different implementation approaches.

The Identity Assurance atomic processes may include personal information or organizational information that is beyond the scope of identity information. There are cases where personal information or organizational information, in addition to identity information, must be validated and verified. The focus of the Identity Assurance compound process is identity, but may be extended to include other personal information or organizational information, as required.

4.5.2 Credential Assurance

The Credential Assurance compound process establishes a measure of certainty (or level of assurance) that a person, organization, or device has maintained control over a credential with which they have been entrusted (or issued) and that the credential has not been compromised (e.g., tampered with, corrupted, modified, stolen, or used without proper authority). The Credential Assurance compound process consists of eight atomic processes. For each atomic process (described in detail in Section 4.4) there is a corresponding **input state**, **output state,** and **conformance criteria** used to standardize the atomic process and assess its integrity. The conformance criteria may also be profiled against **qualifiers** which indicate a requirement that can be traced to a level of assurance, an identity domain requirement, another trust framework requirement, or an applicable business, legal, policy, or regulatory requirement. Figure 9 illustrates the Credential Assurance compound process.

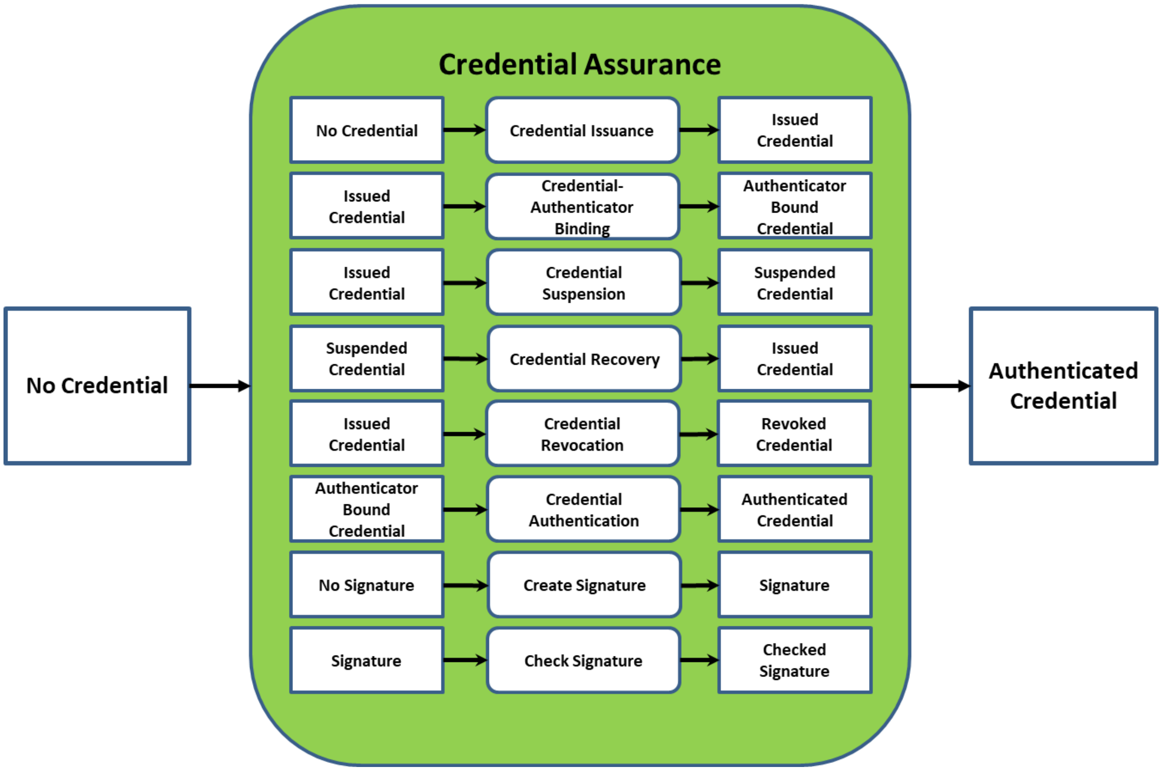


Figure 9: Credential Assurance Compound Process

A single provider may not be responsible for carrying out all the Credential Assurance atomic processes. It may be the case that the atomic processes are carried out by several different providers. For example, *Credential issuance* may be the responsibility of one provider, while *Credential Authentication* may be the responsibility of a different provider. The involvement of several providers may introduce complexity in the assessment and certification process, but the PCTF does not constrain different implementation approaches.

4.5.3 Informed Consent

The Informed Consent compound process obtains meaningful consent from a person[7] for the collection, use, and disclosure of their personal information. The Informed Consent compound process consists of seven atomic processes. For each atomic process (described in detail in Section 4.4) there is a corresponding **input state**, **output state,** and **conformance criteria** used to standardize the atomic process and assess its integrity. The conformance criteria may also be profiled against **qualifiers** which indicate a requirement that can be traced to a level of assurance, an identity domain requirement, another trust framework requirement, or an applicable business, legal, policy, or regulatory requirement. Figure 10 illustrates the Informed Consent compound process.

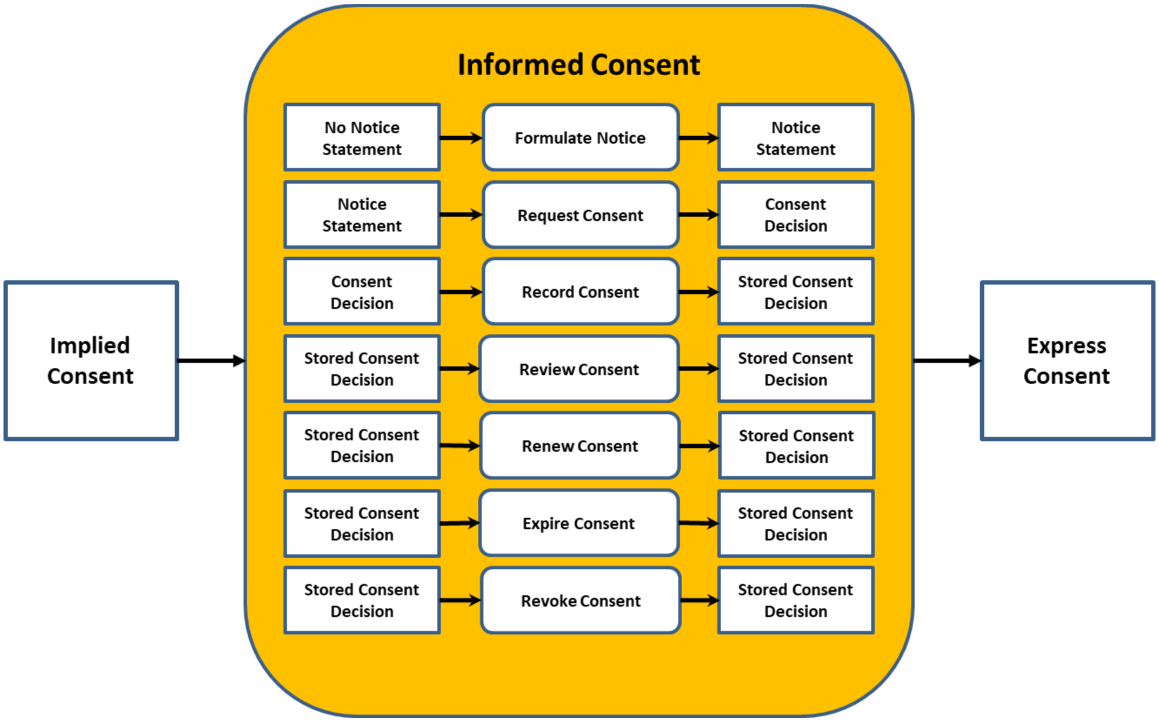


Figure 10: Informed Consent Compound Process

[7] The Informed Consent compound process assumes that the person providing consent has been the subject of both the Identity Assurance and Credential Assurance compound processes, and that consequently the person who is being asked to provide consent has the authority to do so.

A single provider may not be responsible for carrying out all the Informed Consent atomic processes. It may be the case that the atomic processes are carried out by several different providers. For example, *Formulate Notice* may be the responsibility of one provider, while *Request Consent* may be the responsibility of a different provider. The involvement of several providers may introduce complexity in the assessment and certification process, but the PCTF does not constrain different implementation approaches.

4.5.4 Digital Identity (Person) Creation

The Digital Identity (Person) Creation compound process consists of the three compound processes – Identity Assurance, Credential Assurance, and Informed Consent – described previously. These three compound processes combine to create a digital identity for a person. Depending on the digital identity ecosystem, some of these processes may be carried out by different parties at different points in time. Figure 11 illustrates the Digital Identity (Person) Creation compound process.

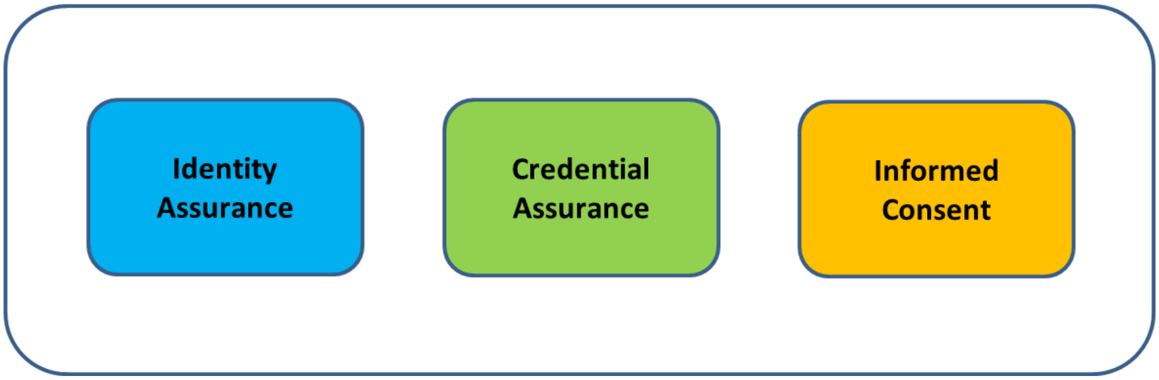


Figure 11: Digital Identity (Person) Creation

4.5.5 Digital Identity (Organization) Creation

The Digital Identity (Organization) Creation compound process consists of the two compound processes – Identity Assurance and Credential Assurance – described previously. These two compound processes combine to create a digital identity for an organization. Depending on the digital identity ecosystem, some of these processes may be carried out by different parties at different points in time.

4.6 Digital Representations as a Set of Proofs

A digital representation can also be conceptualized as a set of PCTF process outputs (proofs). As was noted previously, these proofs are independent of the conveyance method. Figure 12 illustrates the digital identity of a person as a set of proofs.

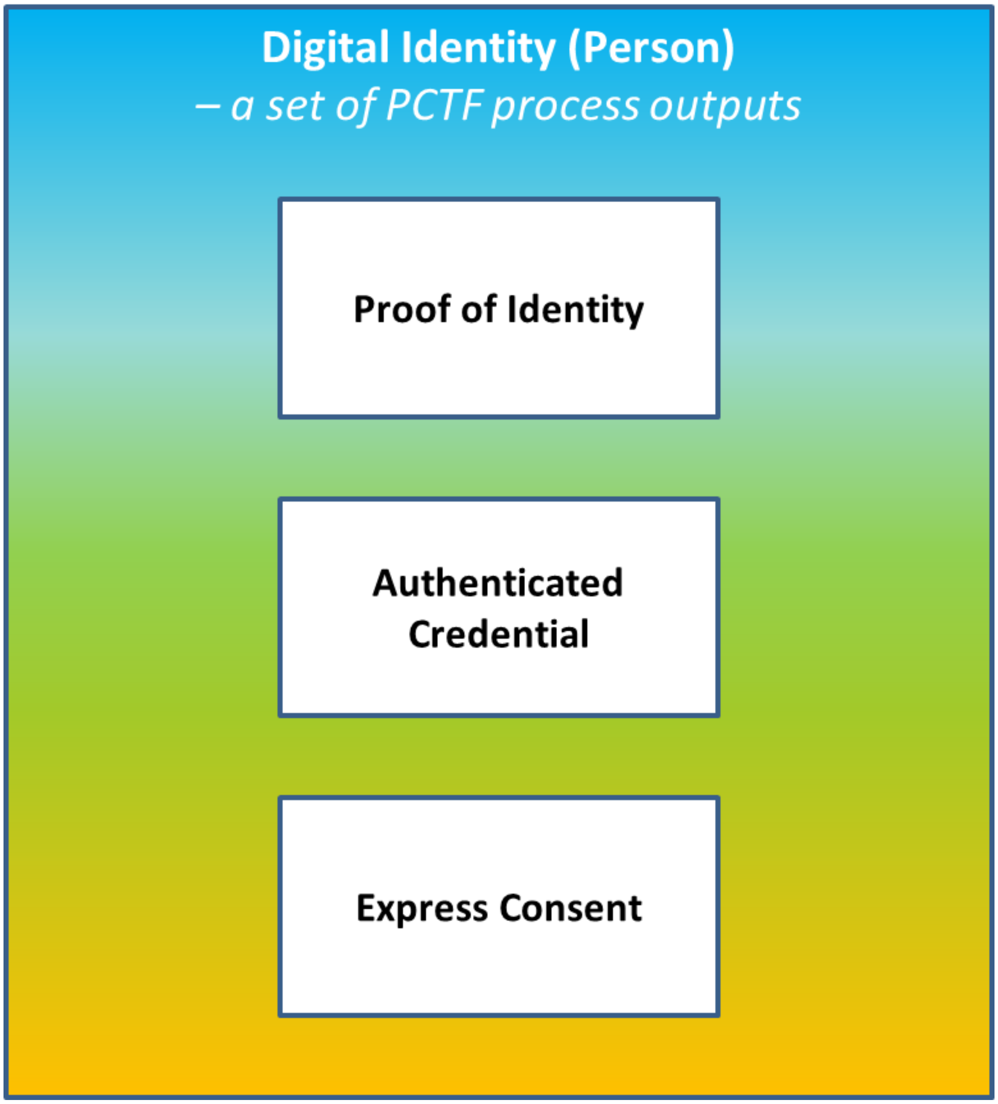


Figure 12: Digital Identity of a Person as a Set of Proofs

4.7 Stakeholders and Roles

4.7.1 Canadian Digital Identity Ecosystem Stakeholders

The Canadian digital identity ecosystem is the vehicle for enabling and growing the digital economy in Canada. The desired characteristics of this digital identity ecosystem are to be open and client-focused where all participants comply with the Pan-Canadian Trust Framework. The result is an interoperable set of networks and services where digital identities and relationships can be provided and consumed across all industries and all levels of government in Canada, thereby enabling program/service providers to focus on core business offerings.

The PCTF does not normatively define stakeholders or roles within the digital identity ecosystem. However, the PCTF can be used to clarify roles and specific stakeholder interests in relation to the provision of PCTF processes, the consumption of PCTF process outputs, and the conveyance of PCTF process outputs between interoperable networks and systems.

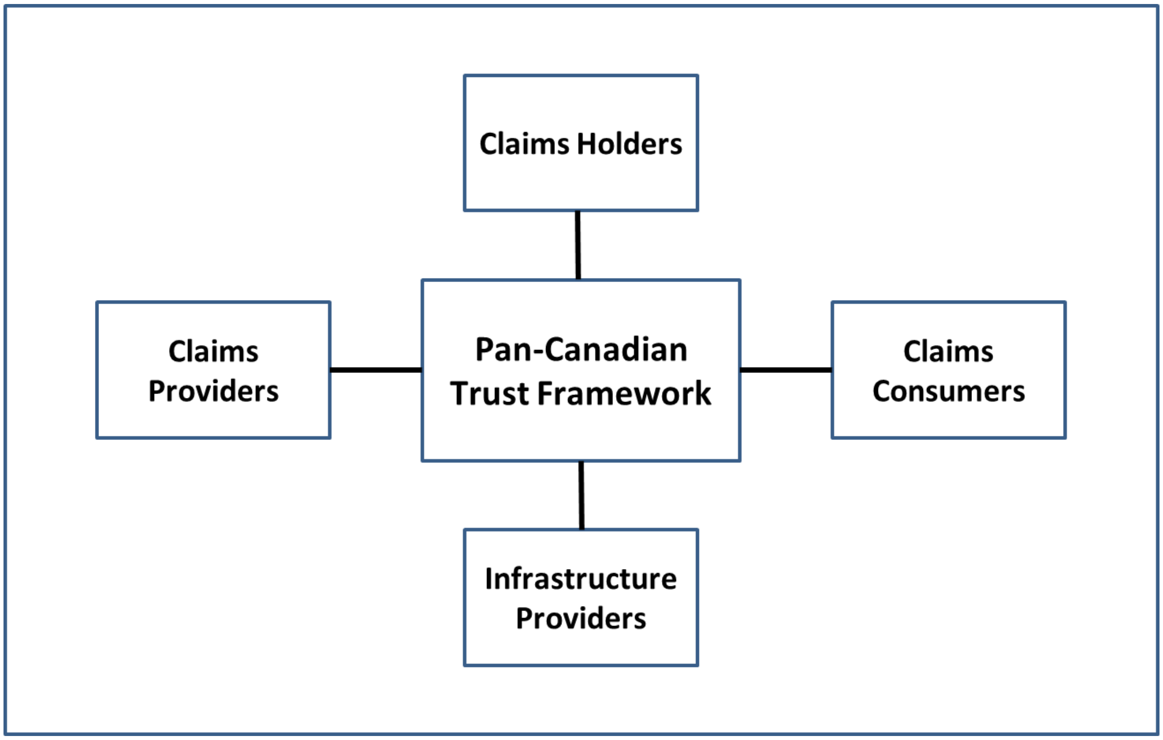


Figure 13: Canadian Digital Identity Ecosystem Stakeholders

Figure 13 illustrates a high-level view of the Canadian digital identity ecosystem stakeholders in relation to the PCTF. The diagram indicates four types of stakeholders:

- **Claims Provider** – An entity (usually an organization) who issues claims to ***claims holders***. Claims providers are also known as ***authoritative parties*** or ***claims issuers***.
- **Claims Holder** – An entity who hold claims which are expressed to and accepted as proofs by ***claims consumers***. Claims holders are usually, but not always, the ***subject*** of a claim.
- **Claims Consumer** – An entity (usually an organization) who consumes claims as a part of their business. Claims consumers accept claims from ***claims holders*** for the purposes of delivering services or administering programs. Claims consumers are also known as ***relying parties*** or ***claims verifiers***.
- **Infrastructure Provider** – An entity (usually an organization) who provides supporting value-added services or acts as intermediaries between parties.

It should be noted that an entity can be more than one type of stakeholder.

The above diagram can assist in developing a common set of stakeholder and role definitions where multiple identity models may coexist within the digital identity ecosystem.

It should also be noted that while the initial focus of the PCTF is to aid in the development of the Canadian digital identity ecosystem, the PCTF can be extended in scope (i.e., new atomic processes can be defined) to incorporate other contextual identity-related claims such as educational or professional claims (e.g., academic degrees, licenses to practice).

4.7.2 PCTF Participant Roles

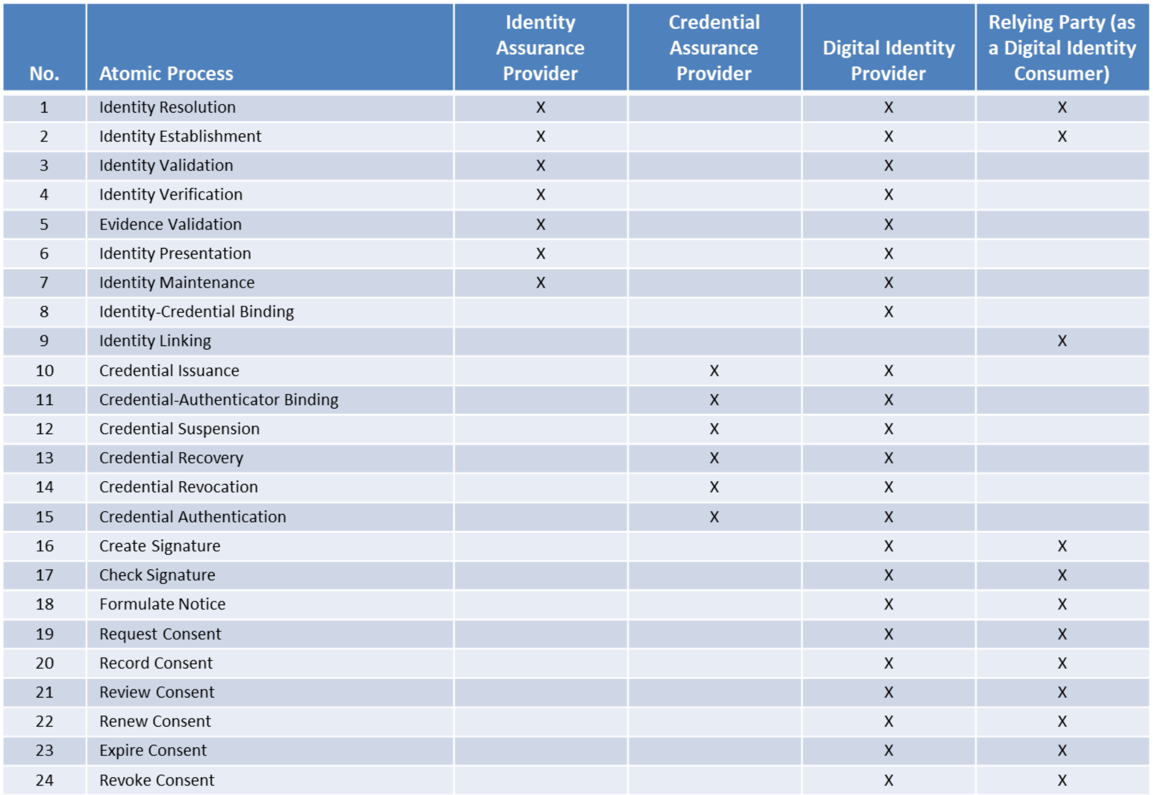
As indicated earlier, the PCTF does not provide normative definition of participant roles, but may be used in identifying roles that may be standardized for the purposes of procurement, standing offers, or supply arrangements. Some PCTF participant roles that have been identified are:

- **Identity Assurance Provider** – A trust framework participant who establishes and manages identities, and provides identity proofing services. An identity assurance provider is a type of claims provider.
- **Credential Assurance Provider** – A trust framework participant who issues electronic credentials for the purposes of authentication, or verifiable credentials for the purposes of proving an identity and/or qualification. A credential assurance provider is a type of claims provider.
- **Digital Identity Provider** – A trust framework participant who provides the end-product of a digital identity. Typically, this is a provincial, territorial, or federal digital identity program that is providing digital identities to another jurisdiction.

These may also be digital Identity providers serving each other within an industry sector. A digital Identity provider is a type of claims provider.

- **Relying Party (as a Digital Identity Consumer)** – A trust framework participant whose core focus is on providing programs and services, where although identity is crucial, it is viewed as an enabler (or cost centre), instead of a strategic business process. A relying party is a type of claims consumer.
- **Digital Identity Owner** – A trust framework participant to whom a digital identity is issued. A digital identity owner is a type of claims holder.

As indicated earlier, these role definitions are not intended to be normative. In many cases there is overlap (and confusion) between existing role definitions, which can be clarified by focusing on who carries out and is responsible for which atomic processes. Figure 14 illustrates four of these participant roles in relation to the atomic processes that they carry out.



No.	Atomic Process	Identity Assurance Provider	Credential Assurance Provider	Digital Identity Provider	Relying Party (as a Digital Identity Consumer)
1	Identity Resolution	X		X	X
2	Identity Establishment	X		X	X
3	Identity Validation	X		X	
4	Identity Verification	X		X	
5	Evidence Validation	X		X	
6	Identity Presentation	X		X	
7	Identity Maintenance	X		X	
8	Identity-Credential Binding			X	
9	Identity Linking				X
10	Credential Issuance		X	X	
11	Credential-Authenticator Binding		X	X	
12	Credential Suspension		X	X	
13	Credential Recovery		X	X	
14	Credential Revocation		X	X	
15	Credential Authentication		X	X	
16	Create Signature			X	X
17	Check Signature			X	X
18	Formulate Notice			X	X
19	Request Consent			X	X
20	Record Consent			X	X
21	Review Consent			X	X
22	Renew Consent			X	X
23	Expire Consent			X	X
24	Revoke Consent			X	X

Figure 14: Atomic Processes by Participant Roles

In terms of providing services, PCTF participant roles are not limited to the three provider roles listed above. Increasingly, there will be providers who specialize in only one or a few of the PCTF atomic processes. These niche providers in the areas of *Identity Presentation* or *Credential Authentication*, for example, once PCTF assessed and certified, can in turn be relied on by other higher-level aggregate providers or by relying parties directly.

4.8 Assessment Approach

The PCTF is used to conduct a comprehensive assessment process of digital identity programs within Canada. The PCTF has been designed to work across multiple contexts, involving numerous parties each having different roles depending on the context.

For example, within the Federal-Provincial-Territorial context, the Government of Canada is a relying party when it accepts a digital identity of a person from a Province or Territory for use by Federal programs and services. The Province or Territory is a digital identity provider and is responsible for ensuring that the individual exists as a real person, is in control of their digital representation, and is acting with express consent. The Government of Canada, as a relying party, uses the PCTF process conformance criteria to ensure that the digital identity as provided by the Province or Territory maps to the right person within each program or service.

As another example, within the Federal-Provincial-Territorial context in relation to organizational identity, the Government of Canada may be a digital identity provider (for corporations) or a relying party that accepts digital identities from a Province or Territory (for sole proprietorships and partnerships) for use by Federal programs and services. The Government of Canada, a Province, or a Territory when acting as a digital identity provider is responsible for ensuring that the organization exists as a legitimate organization and has been registered in the corresponding home jurisdiction in order to conduct its activities. The Government of Canada, as a relying party, uses the PCTF process conformance criteria to ensure that the digital identity as provided by a Province or Territory maps to the right organization and home jurisdiction within each program or service.

4.8.1 Overall Goal

The goal of the PCTF assessment process is to formally assess a digital identity program in order to provide an overall confidence that a relying party, on its own, or on behalf of others, can accept a digital identity. Accepting a digital identity is a decision made by a relying party, who may in turn, need to trace this decision to specific legislative, policy, or regulatory requirements that are outside the scope of the PCTF. The relying party may also need to account for specific program requirements or manage risks that are not the responsibility of the digital identity provider. Ultimately, the PCTF is a tool to assist all parties in understanding who is accountable for what and to clarify specific responsibilities.

At this time, the PCTF assessment process is still in its early stages. Detailed guidance will be developed as the assessment process evolves. The content in the following sections have been derived from key learnings to date and will change as a result of further application.

4.8.2 Project Management, Engagement, and Governance (Approvals).

The PCTF assessment process should be integrated as a discrete work stream within a broader project management process. Typically there are other work streams that include:

- Executive Oversight, Project Governance, and Enterprise Architecture
- Integration and Testing (Technical/UX),
- Security Assessment and Authorization, Privacy Impact Assessments, and Service Agreements
- Communications and Stakeholder Engagement

Team members who are responsible for the PCTF assessment process should be integrated into the larger project team that is responsible for delivering the solution. This is beneficial from two perspectives:

1. The PCTF assessors benefit from the detailed operational and technical knowledge of the other team members; and,
2. The other team members will benefit from the PCTF assessor's perspective – clarifying the 'what' needs to be achieved in order to accept a digital identity using the conformance criteria.

4.8.3 Overview of the Assessment Process

The PCTF assessment process is intended to be adaptable. If necessary, the assessor may wish to tailor the conformance criteria for the specific context. It should be noted that certain conformance criteria (by means of the qualifiers) may be subject to specific governance.

A detailed worksheet has been developed to assist in the PCTF assessment process. This worksheet consolidates the atomic processes and their related conformance criteria into a single spreadsheet to aid in the mapping of existing business processes, and to assist the assessor in easily cross-referencing and synthesizing the data for analysis. The conformance criteria are tabulated with the qualifiers to assist in the selection of the conformance criteria that are applicable to the assessment process.

The first step in the PCTF assessment process is to map the existing business processes to the atomic process definitions. Figure 15 shows a mapping of the business processes of a digital identity provider to the atomic process definitions. This mapping process may also be used by a relying party who may need to augment or risk manage certain atomic processes within their own context.

Once the existing business processes have been mapped, they can be assessed and a determination made against each of the related atomic process conformance criteria. The current formal determinations are:

- **Accepted** – The conformance criteria are met;
- **Accepted with Observation** – The conformance criteria are met, but a dependency or contingency over which the assessed party might not have direct control has been noted;
- **Accepted with Recommendation** – The conformance criteria are met, but a potential improvement or enhancement should be implemented in the future;
- **Accepted with Condition** – The conformance criteria are not met, but the atomic process is accepted due to the demonstration of safeguards, compensating factors, or other assurances in place;
- **Not Accepted** – The conformance criteria are not met; or
- **Not Applicable** – The conformance criteria do not apply.

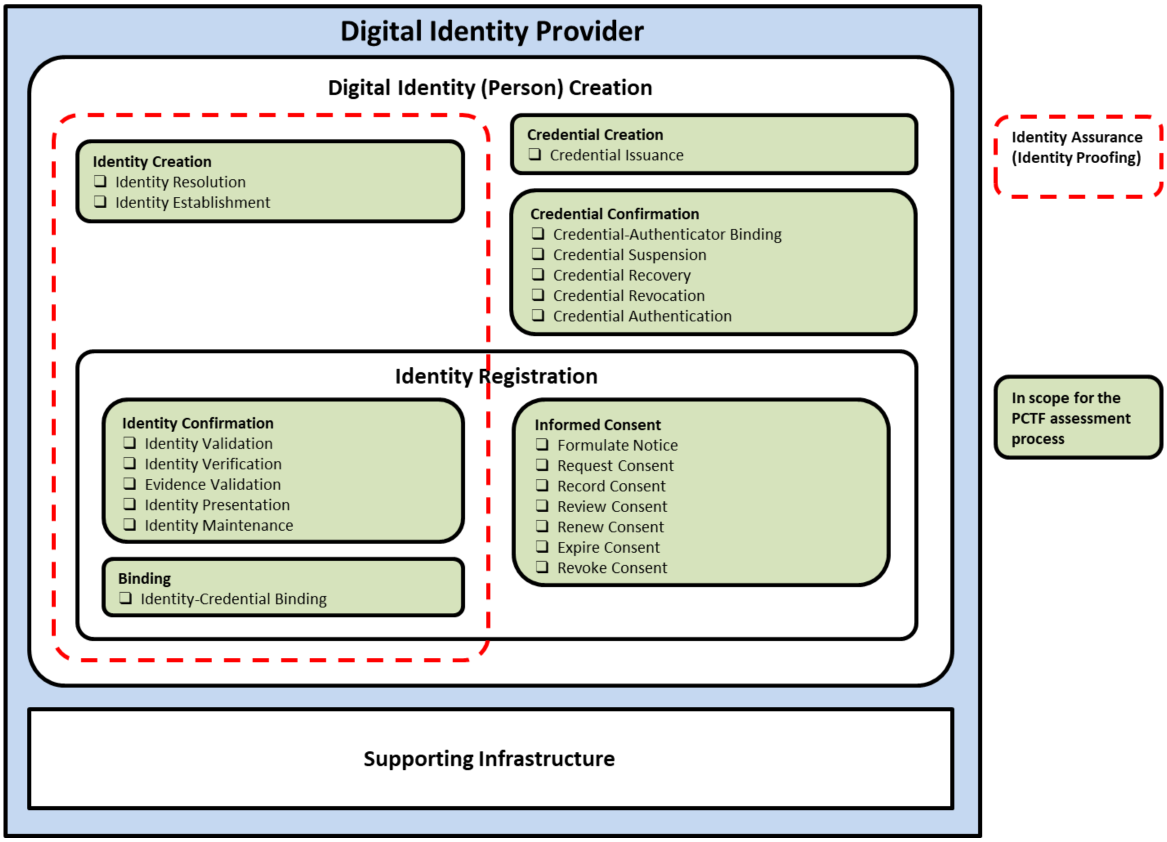


Figure 15: Business Process to Atomic Process Mapping

Evidence to support the analysis and substantiate the determination should be collected and tabulated in a manner that can be easily cross referenced to the applicable conformance criteria.

Upon completion of the assessment process, the relying party may wish to issue a *Letter of Acceptance* for a digital identity. This letter is similar in nature to a *Privacy Impact Assessment* (PIA) or an *Authority to Operate* (ATO) and should include the following:

- Addressed to the person/organization/jurisdiction accountable for being the digital identity provider;
- Signed by the person/organization/jurisdiction accepting the digital identity at a given qualifier level;
- The specific scope or use of the accepted digital identity, including the time period; and,
- An annex listing the specific qualifiers (e.g., levels of assurance), and any observations, conditions, or recommendations arising from the assessment process.

4.8.4 Certification and Accreditation

The International Standards Organization (ISO)[8] defines certification and accreditation as follows:

- **Certification** – the provision by an independent body of written assurance (a certificate) that the product, service, or system in question meets specific requirements.
- **Accreditation** – the formal recognition by an independent body (generally known as an accreditation body) that a certification body operates according to international standards.

It is anticipated that once formalized certification and accreditation programs are developed, independent third parties will be enabled to conduct PCTF assessments. Currently, there are numerous domestic and international standards bodies that have recognized conformity assessment standards and programs. For example, the Standards Council of Canada, a federal Crown corporation, has the mandate to promote voluntary standardization in Canada, where standardization is not expressly provided for by law.

[8] ISO website: https://www.iso.org/certification.html.

It should also be noted, that by design, the PCTF does not assume that a single provider is solely responsible for all of the processes. Therefore, several bodies might be involved in the PCTF assessment process, focusing on different processes, or different aspects (e.g., security, privacy, service delivery). Consideration must be given to how to coordinate several bodies that might need to work together to yield an overall PCTF assessment.

As the PCTF assessment process evolves, consideration will be given to determine which bodies and/or standards are best suited to meet stakeholder requirements and best applied in relation to the PCTF.

Finally, legislation and regulations may change in response to the evolution of the digital identity ecosystem. Lessons learned from implementing solutions based on the PCTF may be considered as valuable input into any potential legislative or regulatory changes.

4.9 Conformance 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 may involve assigning an identifier to a person or organization. The conformance criteria specify that the atomic process must ensure that the identifier that is assigned to the person or organization is unique for a specific population or context.

4.9.1 Qualifiers

Qualifiers may be applied to conformance criteria. Qualifiers help to further indicate a level of confidence, stringency required, or a specific requirement, in relation to another trust framework, an identity domain requirement, or a specific policy or regulatory requirement. Qualifiers can be used to select the applicable conformance criteria to be used in an assessment process. Qualifiers can also be used to facilitate mapping conformance criteria equivalencies across different trust frameworks.

Conformance criteria may have no qualifiers (applicable in all cases), a single qualifier (applicable in certain cases), or several qualifiers (applicable in many cases).

4.9.2 Identity Domain Qualifiers

Qualifiers may be used to qualify conformance criteria that are specific to an identity domain. Currently, there are two identity domain qualifiers: foundational and contextual.

- **Foundational** – conformance criteria that are tied to a specific foundational event (e.g., birth, person legal name change, immigration, legal residency, citizenship, death, organization legal name registration, organization legal name change, bankruptcy) are the exclusive domain of the public sector (more precisely, the Vital Statistics Organizations (VSOs) and Business Registrars of the Provinces and Territories, Immigration, Refugees, and Citizenship Canada (IRCC), and the Federal Corporate Registrar).
- **Contextual** – conformance criteria that are specific to an identity context (contextual identity). For example, in order for evidence of contextual identity to be accepted, the conformance criteria may require that the evidence of contextual identity be issued directly to the recipient with acknowledgement.

4.9.3 Pan-Canadian Levels of Assurance (LOA) Qualifiers

The current version of the PCTF conformance criteria uses the four Pan-Canadian Levels of Assurance (LOA):

- **Level 1**: little or no confidence required
- **Level 2**: some confidence required
- **Level 3**: high confidence required
- **Level 4**: very high confidence required

4.9.4 eIDAS Qualifiers

Qualifiers may be based on the three levels of assurance defined by the European Regulation No 910/2014 on electronic identification and trust services for electronic transactions (known as “eIDAS”):

- **Low**: low degree of confidence
- **Substantial**: substantial degree of confidence
- **High**: high degree of confidence

4.9.5 Vectors of Trust (VoT) Qualifiers

Qualifiers may be based on Vectors of Trust, a proposed IETF standard (RFC 8485, October 2018). Currently, the VoT proposal consists of four components that may be used as qualifiers:

- **Identity Proofing (P)**: describes how likely it is that a given digital identity transaction corresponds to a particular, real-world identity subject
- **Primary Credential Usage (C)**: defines how strongly the primary credential can be verified by the TDIP

- **Primary Credential Management (M)**: conveys information about the expected lifecycle of the primary credential in use, including its binding, rotation, and revocation
- **Assertion Presentation (A)**: defines how well the TDI can be communicated across the network without information leaking to unintended parties and without spoofing

4.9.6 NIST Special Publication 800 63-3 Qualifiers

Qualifiers may be based on levels defined in NIST Special Publication 800-63 Digital Identity Guidelines:

- **Identity Assurance Level (IAL)**: refers to the identity proofing level
- **Authenticator Assurance Level (AAL)**: refers to the authentication process
- **Federation Assurance Level (FAL)**: refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party

4.9.7 Secure Electronic Signature Qualifiers

Part 2 of the Federal *Personal Information Protection and Electronic Documents Act* 7 *(PIPEDA),* defines an electronic signature as "a signature that consists of one or more letters, characters, numbers, or other symbols in digital form incorporated in, attached to, or associated with an electronic document". There are a number of cases where PIPEDA Part 2 is technology specific and requires the use of a particular class of electronic signatures referred to as a ***secure electronic signature*** (which is further defined in the annexed *Secure Electronic Signature (SES) Regulations*).

Secure electronic signature qualifiers may be based on:

- **Signing**: The electronic data has been signed by the person who is identified in, or can be identified through, a digital signature certificate;
- **Algorithms**: Specific asymmetric algorithms are used;
- **Recognition:** The issuing certification authority (CA) is recognized by the Treasury Board of Canada Secretariat; and,
- **Capacity:** Verification that the certification authority has the capacity to issue digital signature certificates in a secure and reliable manner.

5 APPENDIX A: TERMS AND DEFINITIONS

The definitions that follow include authoritative definitions from the *Standard on Identity and Credential Assurance*, definitions found in related guidelines and industry references, and definitions developed by the working group for the purposes of this document.

Term	Definition
anonymous credential	A credential that, while still making an assertion about some property, status, or right of the person, does not reveal the person's identity. A credential may contain identity attributes but still be treated as anonymous if the identity attributes are not recognized or used for identity validation purposes. Anonymous credentials provide persons with a means by which to prove statements about themselves and their relationships with public and private organizations anonymously.
assigned identifier	A numeric or alphanumeric string that is generated automatically and that uniquely distinguishes between persons or organizations without the use of any other identity attributes.
assurance	A measure of certainty that a statement or fact is true.
assurance level	A level of confidence that may be relied on by others.
atomic process	A set of logically related activities that results in the state transition of an object. The object's output state can be relied on as a proof by other processes.
attribute	A property or characteristic associated with an entity. See also "identity attribute".
authenticator	Something that a Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant's identity (also known as "token").
authoritative party	A federation member that provides assurances of credential or identity to other federation members (i.e. "relying parties").
authoritative source	A collection or registry of records maintained by an authority that meets established criteria.

Term	Definition
biological or behavioural characteristic confirmation	A process that compares biological (anatomical and physiological) characteristics in order to establish a link to a person (e.g. facial photo comparison).
biometrics	A general term used alternatively to describe a characteristic or a process. It can refer to a measurable biological (anatomical and physiological) or behavioural characteristic that can be used for automated recognition. It can also refer to automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioural characteristics.
business event	A significant discrete episode that occurs in the life span of a business. By law a business event must be recorded with a government entity and is subject to legislation and regulation. Examples of business events are registration of charter, merger, amalgamation, surrender of charter, and dissolution.
check signature	The process of confirming that the signature for the data is valid.
claims consumer	An entity (usually an organization) who consumes claims as a part of their business. Claims consumers accept claims from *claims holders* for the purposes of delivering services or administering programs. Claims consumers are also known as “relying parties” or “claims verifiers”.
claims holder	An entity who hold claims which are expressed to and accepted as proofs by *claims consumers*. Claims holders are usually, but not always, the “Subject” of a claim.
claims provider	An entity (usually an organization) who issues claims to *claims holders*. Claims providers are also known as “authoritative parties” or “claims issuers”.
client	The intended recipient for a service output. External clients are generally persons (Canadian citizens, permanent residents, etc.) and businesses (public and private sector organizations). Internal clients are generally public service employees and contractors.

Term	Definition
compound process	A set of atomic processes and/or other compound processes that results in a set of state transitions.
conformance criteria	A set of requirement statements that define what is necessary to ensure the integrity of an atomic process.
contextual identity	An identity that is used for a specific purpose within a specific identity context.
create signature	The process of creating an electronic representation where, at a minimum: the person signing the data can be associated with the electronic representation; it is clear that the person intended to sign; the reason or purpose for signing is conveyed; and the data integrity of the signed transaction is maintained, including the original.
credential	A unique physical or electronic object (or identifier) issued to, or associated with, a person, organization, or device (e.g. key, token, document, program identifier).
credential assurance	The assurance that a person, organization, or device has maintained control over the credential with which they have been entrusted (e.g. key, token, document, identifier) and that the credential has not been compromised (e.g. tampered with, corrupted, modified).
credential assurance level	The level of confidence that a person, organization, or device has maintained control over the credential with which they have been entrusted (e.g. key, token, document, identifier) and that the credential has not been compromised (e.g. tampered with, corrupted, modified).
credential assurance provider	A trust framework participant who issues electronic credentials for the purposes of authentication, or verifiable credentials for the purposes of proving an identity and/or qualification. A credential assurance provider is a type of "claims provider".
credential authentication	The process of verifying that a subject has control over their issued credential and that the issued credential is valid (i.e., not suspended or revoked).

Term	Definition
credential-authenticator binding	The process of associating an issued credential with one or more authenticators. This process also includes life-cycle activities such as removing authenticators, binding new authenticators, and updating authenticators (e.g., changing a password, updating security questions and answers, having a new photo taken).
credential federation	A federation established for the purpose of credential management.
credential issuance	The process of creating and assigning a unique credential to a subject (i.e., a person, organization, or device). A credential includes one or more identifiers which may be pseudonymous, and may contain attributes verified by the credential issuer.
credential recovery	The process of transforming a suspended credential back to a usable state (i.e., an issued credential).
credential revocation	The process of ensuring that an issued credential is permanently flagged as unusable.
credential risk	The risk that a person, organization, or device has lost control over the credential with which they have been entrusted.
credential suspension	The process of transforming an issued credential into a suspended credential by flagging the issued credential as temporarily unusable.
digital identity	An electronic representation of a person or organization, used exclusively by that same person or organization, to access valued services and to carry out transactions with trust and confidence.
digital identity owner	A trust framework participant to whom a digital identity is issued. A digital identity owner is a type of “claims holder”.

Term	Definition
digital identity provider	A trust framework participant who provides the end-product of a digital identity. Typically, this is a provincial, territorial, or federal digital identity program that is providing digital identities to another jurisdiction. These may also be digital Identity providers serving each other within an industry sector. A digital identity provider is a type of "claims provider".
digital relationship	An electronic representation of the relationship of one person to another person, one organization to another organization, or a person to an organization.
digital representation	An electronic representation of any entity that can be subject to legislation, policy, or regulations within a context and which may have certain rights, duties, and obligations; or an electronic representation of the relationship between such entities.
document authentication	The process of confirming the authenticity of a document: genuine, counterfeit, forged, etc. Document authentication is achieved by checking the security features of a document, such as secure laminate, holographic images, etc.
documentary evidence	Any physical record of information that can be used as evidence. This is widely understood to mean information written on paper, but the more general definition is preferable.
documented sex	An attribute copied from the "sex" or "gender" indicator on a credential.
electronic or digital evidence	Any data that is recorded or preserved on any medium in, or by, a computer system or other similar device. Examples include database records, audit logs, and electronic word processing documents.
evidence of contextual identity	Evidence of identity that corroborates the evidence of foundational identity and assists in linking the identity information to a person. It may also provide additional information such as a photo, signature, or address. Examples include social insurance records; records of entitlement to travel, drive, or obtain health services;

Term	Definition
	and records of marriage, name change, or death originating from a jurisdictional authority. Evidence of identity that corroborates the evidence of foundational identity and assists in linking the identity information to an organization. It may also provide additional information such as market activity, signature, or address. Examples include business number 9, business number 15, licence to cultivate cannabis, and charity registration number.
evidence of foundational identity	Evidence of identity that establishes core identity information about a person such as given name(s), surname, date of birth, and place of birth. Examples are records of birth, immigration, or citizenship from an authority with the necessary jurisdiction. Evidence of identity that establishes core identity information about an organization such as legal name, date of event, address, status, primary contact. Examples are registration records, certificates of compliance, and incorporation records from an authority with the necessary jurisdiction.
evidence of identity	A record from an authoritative source indicating a person's or organization's identity. There are two categories of evidence of identity: foundational and contextual. See "evidence of foundational identity" and "evidence of contextual identity".
evidence validation	The process of confirming that the evidence presented (whether physical or electronic) can be accepted or be admissible as a proof (i.e., beyond a reasonable doubt, balance of probabilities, and substantial likelihood).
expire consent	The process of suspending the validity of a "yes" consent decision as a result of exceeding an expiration date limit.
federated credentials	The sharing of credential assurances with trusted members of a federation.

Term	Definition
federated identity	The sharing of identity assurances with trusted members of a federation.
federating credentials	The process of establishing a federation in which members share credential assurances with trusted members of the federation.
federating identity	The process of establishing a federation in which members share identity assurances with trusted members of the federation.
federation	A cooperative agreement between autonomous entities that have agreed to relinquish some of their autonomy in order to work together effectively to support a collaborative effort. The federation is supported by trust relationships and standards to support interoperability.
formulate notice	The process of producing a notice statement that describes what personal information is being, or may be, collected; with which parties the personal information is being shared and what type of personal information is being shared; for what purposes the personal information is being collected, used, or disclosed; the risk of harm and other consequences as a result of the collection, use, or disclosure; how the personal information will be handled and protected; the time period for which the notice statement is applicable; and under whose jurisdiction or authority the notice statement is issued.
foundation name	The name of a person or organization as indicated on an official record identifying the person or organization (e.g., provincial/territorial vital statistics record, federal immigration record, provincial/territorial corporate registry record).

Term	Definition
foundation registry	A registry that maintains permanent records of persons who were born in Canada, or persons who were born outside Canada to a Canadian parent, or persons who are foreign nationals who have applied to enter Canada. There are 14 such registries in Canada (the 13 provinces and territories plus Immigration, Refugees, and Citizenship Canada (federal)). A registry that maintains permanent records of organizations that were created and registered in Canada. There are 14 such registries in Canada (the 13 provinces and territories plus Corporations Canada (federal)).
foundational identity	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, citizenship, death, organization legal name registration, organization legal name change, bankruptcy).
gender	The socially constructed roles, behaviours, activities, and attributes that a given society considers appropriate for a male or a female.
identifier	The set of identity attributes used to uniquely distinguish a particular person, organization, or device within a population. (A variant definition derived from the definition found in *The Standard on Identity and Credential Assurance*.)
identity	A reference or designation used to uniquely distinguish a particular person, organization, or device. (A variant definition derived from the definition found in *The Standard on Identity and Credential Assurance*.) There are two types of identity: foundational and contextual. See “foundational identity” and “contextual identity”.
identity assurance	A measure of certainty that a person, organization, or device is who or what it claims to be.
identity assurance level	The level of confidence that a person, organization, or device is who or what it claims to be.

Term	Definition
identity assurance provider	A trust framework participant who establishes and manages identities, and provides identity proofing services. An identity assurance provider is a type of “claims provider”.
identity attribute	A property or characteristic associated with an identifiable person, organization, or device (also known as “identity data element”).
identity claim	An assertion of the truth of something that pertains to a person's or an organization’s identity.
identity context	The environment or set of circumstances within which an organization operates and within which it delivers its programs and services. Identity context is determined by factors such as mandate, target population (i.e. clients, customer base), and other responsibilities prescribed by legislation or agreements.
identity-credential binding	The process of associating an identity with an issued credential.
identity data element	See “identity attribute”.
identity establishment	The process of creating an authoritative record of identity within a program/service population that may be relied on by others for subsequent programs, services, and activities.
identity federation	A federation established for the purpose of identity management.
identity fraud	The deceptive use of personal information in connection with frauds such as the misuse of debit/credit cards or applying for loans using stolen personal information.
identity information	The set of identity attributes that is sufficient to distinguish one entity from all other entities within a program/service population and that is sufficient to describe the entity as required by the program or service. Depending on the context, identity information is either a subset of personal information or a subset of organizational information.

Term	Definition
identity information notification	The disclosure of identity information about a person or an organization by an authoritative party to a relying party that is triggered by a vital event or a business event, a change in their identity information, or an indication that their identity information has been exposed to a risk factor (e.g. the death of the person, a charter surrender, use of expired documents, a privacy breach, fraudulent use of the identity information).
identity information retrieval	The disclosure of identity information about a person or an organization by an authoritative party to a relying party that is triggered by a request from the relying party.
identity information validation	The process of confirming the accuracy of identity information about a person or organization as established by an authoritative party (also known as "identity validation").
identity linking	The process of mapping two or more identifiers to the same identity for the purpose of facilitating identity resolution.
identity maintenance	The process of ensuring that identity information is as accurate, complete, and up-to-date as is required.
identity management	The set of principles, practices, processes, and procedures used to realize an organization's mandate and its objectives related to identity.
identity model	A simplified (or abstracted) representation of an identity management methodology (also known as "identity scheme"). Examples include centralized, federated, and decentralized identity models.
identity presentation	The process of dynamically confirming that a person or organization has a continuous existence over time (i.e., "genuine presence"). This process can be used to ensure that there is no malicious or fraudulent activity (past or present) and to address identity spoofing concerns.
identity proofing	See "identity assurance".

Term	Definition
identity resolution	The process of establishing the uniqueness of a person or organization within a program/service population through the use of identity information.
identity risk	The risk that a person, organization, or device is not who or what it claims to be.
identity scheme	See “identity model”.
identity theft	The preparatory stage of acquiring and collecting someone else's personal information for criminal purposes.
identity validation	The process of confirming the accuracy of identity information about a person or organization as established by an authoritative party (also known as “identity information validation”).
identity verification	The process of confirming that the identity information being presented relates to the person or organization that is making the claim. It should be noted that this process may use personal information or organizational information that is not related to identity.
infrastructure provider	An entity (usually an organization) who provides supporting value-added services or acts as an intermediaries between parties.
knowledge-based confirmation	A process that compares personal or private information (i.e. shared secrets) to establish a person's identity. Examples of information that can be used for knowledge-based confirmation include passwords, personal identification numbers, hint questions, program-specific information, and credit or financial information.
legal name	See “foundation name”, “primary name”.
legal presence	Lawful entitlement to be or reside in Canada.
organization	A legal entity that is not a human being (in legal terms a “juridical person”).
organizational information	Information about an identifiable organization.

Term	Definition
person	A human being (in legal terms a “natural person”) including “minors” and others who might not be deemed to be persons under the law.
personal information	Information about an identifiable person.
personal information notification	The disclosure of personal information about a person by an authoritative party to a relying party that is triggered by the establishment of the person’s identity or a change in their personal information.
personal information retrieval	The disclosure of personal information about a person by an authoritative party to a relying party that is triggered by a request from the relying party.
personal information validation	The confirmation of the accuracy of personal information about a person as established by an authoritative party.
physical possession confirmation	A process that requires physical possession or presentation of evidence to establish a person's or organization’s identity.
preferred name	The name by which a person prefers to be informally addressed.
primary name	The name that a person or organization uses for formal and legal purposes (also known as “legal name”). See also “foundation name”.
proof	Evidence or argument establishing or helping to establish the truth or correctness of a statement.
record consent	The process of persisting a notice statement and the subject’s related consent decision, to storage. In addition, information about the subject, the version of the notice statement that was presented, the date and time that the notice statement was presented, and, if applicable, the expiration date for the consent decision may be stored. Once the consent information has been stored, a notification on the consent decision made is issued to the relevant parties to the consent decision.

Term	Definition
relying party	A federation member who relies on assurances of credential or identity from other federation members (i.e. “authoritative parties”).
renew consent	The process of extending the validity of a “yes” consent decision by means of increasing an expiration date limit.
request consent	The process of presenting a notice statement to the subject (i.e., the natural person to whom the personal information in question pertains) and asking the subject to agree to provide consent (“Yes”) or decline to provide consent (“No”) based on the contents of the notice statement, resulting in either a “yes” or “no” consent decision.
review consent	The process of making the details of a stored consent decision visible to the subject or to an authorized reviewer.
revoke consent	The process of suspending the validity of a “yes” consent decision as a result of an explicit withdrawal of consent by the subject (i.e., a “yes” consent decision is converted into a “no” consent decision).
risk	The uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives.
sex	The biological characteristics that define a human being as female or male. These sets of biological characteristics are not mutually exclusive as there are persons who possess both female and male characteristics.
signature	An electronic representation where, at a minimum: the person signing the data can be associated with the electronic representation, it is clear that the person intended to sign, the reason or purpose for signing is conveyed, and the data integrity of the signed transaction is maintained, including the original.
token	See “authenticator”.

Term	Definition
trust	A firm belief in the reliability or truth of a person, organization, or device.
trust framework	A set of agreed on principles, definitions, standards, specifications, conformance criteria, and assessment approach.
trusted referee confirmation	A process that relies on a trusted referee to establish a link to a person. The trusted referee is determined by program-specific criteria. Examples of trusted referees include guarantors, notaries, and certified agents.
vital event	A significant discrete episode that occurs in the life span of a person. By law a vital event must be recorded with a government entity and is subject to legislation and regulation. Examples of vital events are live birth, foetal death (i.e. stillbirth), adoption, legitimation, recognition of parenthood, marriage, annulment of marriage, legal separation, divorce, and death.

6 APPENDIX B: IDENTITY MANAGEMENT OVERVIEW

This appendix provides a general overview of specific topics in identity management. Additional information can be found in the *Guideline on Identity Assurance* [TBS, 2015].

6.1 Identity

6.1.1 Real-World Identity

> "Identity is how we recognize, remember, and ultimately respond to specific people and things…It helps us recognize friends, families, and threats; it enables remembering birthdays, preferences, and histories; it gives us the ability to respond to each individual as their own unique person.
>
> …Our identity is bigger than our digital selves. Our identities existed before and continue to exist independent of any digital representation. Digital identities are simply tools which help organizations and individuals manage real-world identity."
>
> – *A Primer on Functional Identity* by Joe Andrieu[9]

6.1.2 Identity in Identity Management

Identity in the domain of identity management has a much narrower scope than real-world notions of identity. In identity management, identity is defined as a reference or designation used to uniquely distinguish a particular person, organization, or device.

An identity must be unique[10]. This means that each person and organization can be distinguished from all other persons and organizations and that, when required, each person and organization can be uniquely identified. The uniqueness requirement ensures that a program or service can be delivered to a specific person or organization and that a program or service is delivered to the right person or organization.

6.2 Defining the Population

In the Canadian context, the universe of persons is defined as all living persons resident in or visiting Canada, as well as all deceased persons, for whom an identity has been established in Canada. The universe of organizations is defined as all organizations registered and operating in Canada, as well as inactive organizations, for which an identity has been established in Canada. Those persons or organizations who fall within the mandate of a program or service constitute the population of the program or service[11].

[9] The full text of the article can be found at: http://bit.ly/FunctionalIdentityPrimer.

[10] This is one of the requirements for establishing an identity assurance level. See Appendix C of the *Standard on Identity and Credential Assurance* [TBS, 2013].

[11] The characteristics of a program/service population are a key factor in determining identity context. See the next section.

In the public sector, the following are some examples of program/service populations in Canada:

- Persons who were born in Alberta
- Persons who are required to file a federal income tax return
- Persons who are licensed to drive in Quebec
- Persons who are military veterans
- Persons who are covered by provincial health insurance in Ontario
- Organizations which are licensed to cultivate cannabis in Canada
- Organizations which are required to register with FINTRAC
- Organizations which are licensed to cut timber in British Columbia
- Organizations which are subject to the supervision of the Office of the Superintendent of Financial Institutions
- Organizations which are licensed to construct and operate oil and gas facilities in Saskatchewan

6.3 Defining the Identity Context

In delivering their programs and services, program/service providers operate within a certain environment or set of circumstances, which in the domain of identity management is referred to as the identity context. Identity context is determined by factors such as mandate, target population (i.e., clients, customer base), and other responsibilities prescribed by legislation or agreements.

Understanding and defining the identity context assists program/service providers in determining what identity information is required and what identity information is not required. Identity context also assists in determining commonalities with other program/service providers, and whether identity information and assurance processes can be leveraged across contexts.

The following considerations should be kept in mind when defining the identity context of a given program or service:

- Intended recipients of the program or service – recipients may be external to the program/service provider (e.g., citizens, non-Canadians, businesses, non-profit organizations), or internal to the program/service provider (e.g., employees, departments)
- Size, characteristics, and composition of the client population
- Commonalities with other programs and services (i.e., across program/service providers)

- Program/service providers with similar mandates
- Use of shared services

6.4 Determining Identity Information Requirements

A property or characteristic associated with an identifiable person or organization is referred to as an *identity attribute* or an *identity data element*. Examples of identity attributes include *name*, *date of birth*, and *sex*. For any given program or service, identity information is the set of identity attributes that is both:

- Sufficient to distinguish between different persons or organizations within the program/service population (i.e., achieve the uniqueness requirement for identity); and
- Sufficient to describe the person or organization as required by the program or service.

Identity information is a strict subset of the much broader set of information referred to as either personal information ("information about an identifiable person") or organizational information ("information about an identifiable organization").

When determining the identity information requirements for a program or service, program/service providers need to distinguish between identity information and program-specific personal information, as these can overlap[12]. For example, *date of birth* can be used to help achieve identity uniqueness (i.e., it is used as identity information) – but *date of birth* can also be used as an age eligibility requirement (i.e. it is used as program-specific personal information). When overlap between identity information and program-specific personal information occurs, it is a good practice to describe both purposes. This ensures that the use of identity information is consistent with the original purpose for which the identity information was obtained and that it can be managed separately or additionally protected by appropriate security and privacy controls. Program/service providers are advised to reduce the overlap between identity information and program-specific personal information as much as possible.

[12] This is usually not an issue for organizational information.

6.4.1 Identifier

The set of identity attributes that is used to uniquely distinguish a particular person or organization within a program/service population is referred to as an *identifier*. This set of attributes is usually a subset of the identity information requirements of a program or service.

Different sets of identity attributes may be specified as an identifier depending on program or service requirements and, in some cases, legislation. For example, one program may specify *name* and *date of birth* as the identifier set of identity attributes. Another program may specify *name*, *date of birth*, and *sex* as the identifier set of identity attributes. Yet another program may use an *assigned identifier* (such as a health insurance number or a business number) as the identifier set of identity attributes.

When determining the set of identity attributes to be used as an identifier, the following factors should be considered:

- **Universality** – Every person or organization within the program/service population must possess the identifier set of identity attributes. However, even when an identity attribute is universal, widespread missing or incomplete values for the identity attribute may render it useless as part of an identifier set. For example, many dates of birth for persons born outside of Canada consist only of the year or the year and the month.
- **Uniqueness** – The values associated with the identity attributes must be sufficiently different for each person or organization within the program/service population that the persons or organizations within the program/service population can be distinguished from one another. For example, date of birth information by itself is insufficient to distinguish between persons in a population because many people have the same birthdate.
- **Constancy** – The values associated with the identity attributes should vary minimally (if at all) over time. For example, having address information in the identifier set is problematic because a person's address is likely to change several times in their lifetime.
- **Collectability** – Obtaining a set of values for the identity attributes should be relatively easy. For example, human DNA sequences are universal, unique, and very stable over time, but they are somewhat difficult to obtain.

6.4.2 Assigned Identifier

It is generally agreed that *name* and *date of birth* comprise the minimum set of identity attributes required to constitute an identifier for a person. Analyses[13] have shown that a combination of *name (surname* + *first given name*) and full *date of birth* will distinguish between upwards of 96% of the persons in any population. While adding other identity attributes (e.g. *sex*, *place of birth*) to the set provides some marginal improvement, no combination of identity attributes can guarantee absolute uniqueness for 100% of a given population. Consequently, due to the potential for identity overlap in whatever residual percentage of the population remains, program/service providers employ the use of an *assigned identifier*. An assigned identifier is an artificial identity attribute that is used solely for the purpose of providing identity uniqueness. It consists of a numeric or alphanumeric string that is generated automatically and is assigned to a person or organization at the time of identity establishment. However, before an assigned identifier can be associated with a person or organization, the uniqueness of the person's or organization's identity within the relevant population must first be established (i.e. identity resolution must be achieved (see next section)) through the use of other identity attributes (e.g. *name*, *date of birth*, etc.). Therefore, the use of an assigned identifier does not eliminate the need for traditional identity resolution techniques, but it does reduce the need to a one-time only occurrence for each person or organization within a population.

Once associated with a person or organization, an assigned identifier uniquely distinguishes that person or organization from all other persons or organizations in a population without the use of any other identity attributes. Examples of assigned identifiers include birth registration numbers, business numbers, driver's license numbers, social insurance numbers, and customer account numbers. The following considerations apply to the use of assigned identifiers:

- Assigned identifiers may be kept internal to the program that maintains them.
- Assigned identifiers maintained by one program may be provided to other programs so that those programs can also use the assigned identifier to distinguish between different persons or organizations within their program/service population; however, there may be restrictions on this practice due to privacy considerations or legislation.
- Certain assigned identifiers may be subject to legal and policy restrictions. For example, the Government of Canada imposes restrictions on the collection, use, retention, disclosure, and disposal of the social insurance number.

[13] NASPO IDPV Project, Report of the IDPV Identity Resolution Project, February 17, 2014

6.5 Identity Resolution

Identity resolution is defined as the establishment of the uniqueness of a person or organization within a program/service population through the use of identity information. A program or service defines its identity resolution requirements in terms of identity attributes; that is, it specifies the set of identity attributes that is required to achieve identity resolution within its population. Since the identifier is the set of identity attributes that is used to uniquely distinguish a unique and particular person or organization within a program/service population, the identifier is the means by which identity resolution is achieved.

Since identity resolution requirements may differ from one program or service to another, the responsibilities of authoritative parties and relying parties in respect to identity resolution are the following:

- Both authoritative parties and relying parties must establish the identity resolution requirements of their program/service populations.
- An authoritative party must publish the identity resolution requirements of its program/service population.

6.6 Ensuring the Accuracy of Identity Information

Identity information must be accurate, complete, and up to date[14]. Accuracy ensures the quality of identity information. It ensures that the information represents what is true about a person or organization, and that it is as complete and up to date as necessary.

For identity information to be considered accurate, three requirements must be met:

- **The identity information is correct and up to date.** Identity information, due to certain life events (e.g. marriage), may change over time. Ongoing updates to identity information may be required; otherwise, it becomes incorrect.
- **The identity information relates to a real person or organization**. Identity information must be associated with a person or organization which actually exists or existed at some point in time.
- **The identity information relates to the correct person or organization.** In large populations, persons or organizations may have the same or similar identity information as other persons or organizations. While the requirement for identity uniqueness addresses this issue, the possibility of relating identity information to the wrong person or organization still remains.

[14] This is one of the requirements for establishing an identity assurance level. See Appendix C of the *Standard on Identity and Credential Assurance* [TBS, 2013].

It is the responsibility of program/service providers to ensure the accuracy of the identity information that is used within their programs and services. The accuracy of identity information can be ensured by using an authoritative source. There are three methods by which this can be achieved:

- On an as needed basis, request confirmation from an authoritative source that the identity information is accurate. This process is referred to as *identity information validation*. For example, a person's sex might be electronically validated using a provincial vital statistics registry[15].
- On an as needed basis, request the identity information from an authoritative source. This process is referred to as *identity information retrieval*. For example, a person's place of birth might be electronically retrieved from the federal registry of persons born abroad.
- Subscribe to a notification service provided by an authoritative source. This process is referred to as *identity information notification*. For example, death notifications might be received from a provincial vital statistics registry.

These methods can be used independently or in combination, and an effective strategy usually requires the use of all three.

If ensuring the accuracy of identity information by means of an authoritative source is not feasible, other methods may be employed, such as corroborating identity information using one or more instances of evidence of identity.

[15] Factors such as spelling and phonetic variations, name changes, and different character sets can make the validation of some identity data elements problematic. Such factors may make it difficult to demand exact matching. Government organizations may need to use approximate or statistical matching methods to determine if identity information acceptably matches an authoritative record. However, it should be noted that **an *identifier* is always subject to an exact match**. In cases where the integrity of an identifier can be determined using a mathematical algorithm (e.g. a checksum calculation for an assigned identifier), these methods should be applied.

7 APPENDIX C: PERSONS AND ORGANIZATIONS

This appendix provides some additional background information on the nature of persons and organizations from a strictly legal perspective.

7.1 Legal Entities

In law there are of two kinds of legal entities: human beings which are known as *natural persons* (also called *physical persons*), and non-human *juridical persons* – also called *juridic persons*, *juristic persons*, *artificial persons*, *legal persons*, or *fictitious persons* (Latin: *persona ficta*) – such as a corporation, a firm, a business or non-business group, or a government agency, etc., that are treated in law as if they were natural persons. Note, however, that the use of the term *legal person* to represent only a non-human legal entity is incorrect. In law, both human and non-human legal entities are recognized as legal persons that have certain privileges and obligations such as the legal capacity to enter into contracts, to sue, and to be sued.

Human beings acquire *legal personhood* when they are born (or even before (i.e., a foetus) in some jurisdictions). Juridical persons acquire legal personhood when they are incorporated in accordance with law. The term *legal personality* is used to describe the characteristic of having acquired the status of legal personhood.

Legal personhood is a prerequisite to *legal capacity* i.e., the ability of any legal person to transact (enter into, amend, transfer, etc.) rights and obligations. For example, in international law legal personality is a prerequisite for an international organization to be able to sign international treaties in its own name.

7.2 Juridical Persons

A juridical person has a legal name and has certain rights, protections, privileges, responsibilities, and liabilities in law, similar to those of a natural person. The concept of a juridical person is a fundamental *legal fiction*. It is pertinent to the philosophy of law, as it is essential to laws affecting a corporation (i.e., corporate law).

Juridical personality is the characteristic of a non-living legal entity regarded by law to have the status of legal personhood.

Juridical personhood allows one or more natural persons (*universitas personarum*) to act as a single entity (a body corporate) for legal purposes. In many jurisdictions, juridical personality allows that entity to be considered under law separately from its individual members (for example in a company limited by shares, its shareholders). A juridical person may sue and be sued, enter contracts, incur debt, and own property. A juridical person may also be subjected to certain legal obligations, such as the payment of taxes. An entity with juridical personality may shield its members from personal liability.

In some common law jurisdictions a distinction is drawn between a *corporation aggregate* (such as a company, which is composed of a number of members) and a *corporation sole*, which is a public office of legal personality separated from the individual holding the office. Historically, most corporations sole were ecclesiastical in nature (for example, the office of the Archbishop of Canterbury is a corporation sole), but a number of other public offices are now formed as corporations sole.

The concept of juridical personality is not absolute. "Piercing the corporate veil" refers to looking at the individual natural persons acting as *agents* involved in a company action or decision. This may result in a legal decision in which the rights or duties of a corporation or public limited company are treated as the rights or liabilities of that corporation's members or directors.

7.3 History of Juridical Persons

The concept of legal personhood for organizations of people (juridical personhood) is at least as old as Ancient Rome: a variety of collegial institutions enjoyed the benefit under Roman law.

The doctrine of juridical personhood has been attributed to Pope Innocent IV who helped to spread the idea of persona ficta. In canon law, the doctrine of persona ficta allowed monasteries to have a legal existence that was apart from the monks, simplifying the difficulty in balancing the need for such groups to have infrastructure though the monks themselves took vows of personal poverty. Another effect of this was that as a fictional person, a monastery could not be held guilty of delict[16] due to not having a soul, helping to protect the organization from non-contractual obligations to surrounding communities. This effectively moved such liability to individuals acting within the organization while protecting the structure itself, since individuals were considered to have a soul and therefore capable of being guilty of negligence.

In the common law tradition, only a natural person could sue or be sued. This was not a problem in the era before the Industrial Revolution, when the typical business venture was either a sole proprietorship or partnership – the owners were simply liable for the debts of the business. A feature of the corporation, however, is that the owners/shareholders enjoyed limited liability – the owners were not liable for the debts of the company. Thus, when a corporation breached a contract or broke a law, there was no remedy, because limited liability protected the owners and the corporation wasn't a legal person subject to the law. There was no accountability for corporate wrongdoing.

[16] Delict is a term in civil law jurisdictions for a civil wrong consisting of an intentional or negligent breach of duty of care that inflicts loss or harm and which triggers legal liability for the wrongdoer.

To resolve this issue, the legal personality of a corporation was established to include five legal rights: the right to a common treasury or chest (including the right to own property), the right to a corporate seal (i.e., the right to make and sign contracts), the right to sue and be sued (to enforce contracts), the right to hire agents (employees), and the right to make by-laws (self-governance).

Since the 19th century, legal personhood of an organization has been further construed to make it a citizen, resident, or domiciliary of a state. The concept of a juridical person is now central to Western law in both common-law and civil-law countries, but it is also found in virtually every legal system.

7.4 Examples of Juridical Persons

Some examples of juridical persons include:

- Corporation: A body corporate created by statute or charter. A corporation aggregate is a corporation constituted by two or more natural persons. A corporation sole is a corporation constituted by a single natural person, in a particular capacity, and that person's successors in the same capacity, in order to give them some legal benefit or advantage, particularly that of perpetuity, which a natural person cannot have. Examples of corporations sole are a religious officiant in that capacity, or The Crown in the Commonwealth realms. Municipal corporations (municipalities) are "creatures of statute". Other organizations may be created by statute as legal persons including European economic interest groupings (EEIGs).

- Partnership: An aggregate of two or more natural persons to carry on a business in common for profit and created by agreement. Traditionally, partnerships did not have continuing legal personality, but many jurisdictions now treat them as having such.

- Company: A form of business association that carries on an industrial enterprise. A company is often a corporation, although a company may take other forms, such as a trade union, an unlimited company, a trust, or a fund. A limited liability company – whether it is a private company limited by guarantee, a private company limited by shares, or a public limited company – is a business association having certain characteristics of both a corporation and a partnership. Different types of companies have a complex variety of advantages and disadvantages.

- Cooperative (co-op): A business organization owned and democratically operated by a group of natural persons for their mutual benefit.

- Unincorporated association: An aggregate of two or more natural persons which are treated as juridical persons in some jurisdictions but not others.

- Sovereign states are juridical persons.
- In the international legal system, various organizations possess legal personality. These include intergovernmental organizations (e.g., the United Nations, the Council of Europe) and some other international organizations (including the Sovereign Military Order of Malta, a religious order).
- The European Union (EU) has had legal personality since the Lisbon Treaty entered into force on December 1, 2009. That the EU has legal personality is a prerequisite for the EU to join the European Convention on Human Rights (ECHR). However, in 2014, the EU decided not to be bound by the rulings of the European Court of Human Rights.
- Temples, in some legal systems, have separate legal personality.

Not all organizations have legal personality. For example, the board of directors of a corporation, legislature, or governmental agency typically are not legal persons in that they have no ability to exercise legal rights independent of the corporation or political body of which they are a part.

7.5 Legal Entity Information

In Canada, the treatment and handling of personal information (information about an identifiable person) and organizational information (information about an identifiable organization) differs significantly. This is shown in the following table:

Legislative and Regulatory Provisions	**Scope and Application**	
	Personal Information	**Organizational Information**
Privacy	All	N/A
Protection	All	Some

8 APPENDIX D: BIBLIOGRAPHY

Organizations

1. Canadian Joint Councils (CJC)
   - Canadian Joint Councils' Digital Identity Priority: Public Policy Recommendations (2018)
2. Communications Security Establishment (CSE)
   - User Authentication Guidance for Information Technology Systems (2018)
3. Digital Identity and Authentication Council of Canada (DIACC)
   - Pan-Canadian Trust Framework Overview (August 2016)
   - Verified Person Component Overview (May 2017)
   - Verified Login Component Overview (January 2018)
   - Notice and Consent Component Overview (April 2019)
   - Pan-Canadian Trust Framework Model Overview (February 2019)
4. Identity Management Sub-Committee (IMSC)
   - Pan-Canadian Assurance Model
   - Pan-Canadian Paper on Trusting Identities
5. Office of the Privacy Commissioner of Canada (OPC)
   - Guidelines for Obtaining Meaningful Consent (May 2018)
6. Treasury Board of Canada Secretariat (TBS)
   - Federating Identity Management in the Government of Canada (2011)
   - Guideline on Defining Authentication Requirements (2012)
   - Standard on Identity and Credential Assurance (2013)
   - Guideline on Identity Assurance (2015)
   - Directive on Identity Management (2019)
7. World Bank (WB)
   - ID4D Practitioner's Guide (2019)

Individuals

1. Joe Andrieu
   - A Primer on Functional Identity (2018)

9 APPENDIX E: THEMATIC ISSUES

The IMSC PCTF Working Group has identified several high-level thematic issues that the group will address in the short to medium term.

Thematic Issue 1: Defining the PCTF

It is becoming clear that the PCTF is a set of agreed-on concepts and criteria as opposed to being some sort of ‘standard’. Instead, it is a framework that helps to situate existing standards (both business and technical) and relevant policy, guidance, and practices. This is certainly the case at the Federal level where the atomic processes and their associated conformance criteria have been mapped to the Federal government’s policy instruments, supporting guidelines, and technical interface standards. We need to ensure that this definition of the PCTF as a detailed policy framework is communicated clearly and consistently within the document.

Thematic Issue 2: Digital Relationships

We need to work on expanding our treatment and coverage of digital relationships within the document – currently, that coverage is not much more than a definition and a set of placeholders.

Thematic Issue 3: The Evolving State of Credentials and Claims

We now find ourselves in the middle of some very interesting developments in the areas of digital credentials and verifiable claims. There is a sea-change happening in the industry where there is a movement from ‘information-sharing’ to ‘presenting digital claims’. There is also some good standards work going on at the W3C relating to verifiable credentials and decentralized identifiers.

Due to these new developments, we are now seeing the possibility that the traditional intermediated services (such as centralized/federated login providers) may disappear due to new technological advancements. This may not happen in the near future, but we are currently adjusting the PCTF model to incorporate the broader notion of a ‘verifiable credential’ (more than a login) and are generalizing it to allow physical credentials (e.g., birth certificates, driver’s licences) to evolve digitally within the model.

We are not sure that we have the model completely right (yet), but nonetheless Canada seems to be moving into the lead in understanding the implications of applying these technologies at ecosystem-scale (both public and private). As such, we are getting inquiries about how the PCTF might facilitate the migration to digital ecosystems and to new standards-based digital credentials, open-standards verification systems, and international interoperability.

Thematic Issue 4: Stakeholders, Roles, and Actors

The current version of the PCTF still reflects differences in perspective in regards to who or what are the stakeholders, roles, and actors in the PCTF. This is due to the PCTF model's anticipated shift towards verifiable claims, verifiable credentials, and decentralized identifiers (see Thematic Issue 3). As we resolve Thematic Issue 3, the definition and delineation of PCTF stakeholders, roles, and actors should become clearer.

Thematic Issue 5: Informed Consent

Informed consent is an evolving area and we don't think the PCTF currently captures all the issues and nuances surrounding this topic. We have incorporated material from the DIACC and we have adjusted this material for public sector considerations. But with the recent publication of the Canada Digital Charter there is debate in the consent area, especially in what might need to change in legislation. Shortly, discussion papers will be released on how Canada might update legislation relating to privacy, consent, and digital identity. We fully expect the notion of consent to change, but for the meantime, we feel that we have enough clarity in the PCTF to proceed with assessments – but we are ready to make changes if necessary.

Thematic Issue 6: Scope of the PCTF

Some have suggested that the scope of the PCTF should be broadened to include academic qualifications, professional designations, etc. We are currently experimenting with pilots in these areas with other countries. We have anticipated extensibility through the generalization of the PCTF model and the potential addition of new atomic and compound processes. Keep in mind however, that digital identity is a very specific but hugely important use case that we need to get right first. We are not yet ready to entertain a broadened scope for the PCTF into other areas, but soon we will.

Thematic Issue 7: Additional Detail

Many questions have been asked about the current version of this document in regards to the specific application of the PCTF. While we have a good idea, we still don't have all of the answers. Much of this detail will be derived from the actual application of the PCTF (as was done with Alberta previously). The PCTF is a framework and, as it is applied, it will likely be supplemented by detailed guidance separate from the PCTF itself. We don't know exactly what this additional material will look like until we learn more through the application of the current PCTF.