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

VERSION 1.1

Document Version:	0.4
Document Status:	Consultation Draft
Date:	2020-06-02
Security Classification:	UNCLASSIFIED

12

13 # DOCUMENT VERSION CONTROL

Version Number	Date of Issue	Author(s)	Brief Description
0.1	2019-10-10	PSP PCTF WG	Consultation Draft
0.2	2019-10-31	PSP PCTF WG	Consultation Draft
0.3	2020-02-20	PSP PCTF WG	Consultation Draft
0.4	2020-06-02	PSP PCTF WG	Consultation Draft

14

15

16

17

18

TABLE OF CONTENTS

LIST OF FIGURES

127

128

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:

- **Section 1** describes the purpose and audience of the document;
- **Section 2** describes the main elements of the PCTF; and
- **Sections 3 through 9** provide various appendices that cover terms and definitions, discussions on selected topics related to the PCTF, a list of issues that will be resolved in future versions of the document, and a bibliography.

The Pan-Canadian Trust Framework will facilitate the transition to a digital ecosystem for citizens and residents of Canada. A Canadian digital ecosystem will increase efficiency and secure interoperability between existing business processes, such as open banking, business licencing, and public sector 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 the various communities who need to trust digital identities. The PCTF is defined in a way that encourages innovation and the evolution of the digital ecosystem. The PCTF allows for the interoperability of different platforms, services, architectures, and technologies.

The PCTF defines two types of *digital representations* that are essential for the development of the digital ecosystem:

1. *Digital identities* of entities such as persons, organizations, and devices; and
2. *Digital relationships* between entities.

The PCTF supports the acceptance of digital identities and digital relationships by defining a set of discrete process patterns, known as *atomic processes*. These atomic processes can be mapped to existing business processes, independently assessed using conformance criteria[1], and certified to be trusted and interoperable within the digital ecosystem.

[1] The conformance criteria are maintained in a separate document.

160
161
162
163
164

1 INTRODUCTION

The purpose of this document is to describe the public sector profile of the Pan-Canadian Trust Framework (PCTF)[2].

The audience for this document includes:

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

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

[2] Development of the public sector profile of the Pan-Canadian Trust Framework is a collaborative effort led by 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 Public Sector Profile PCTF Working Group (PSP PCTF WG) for the purposes of discussion and consultation, and its contents have not yet been endorsed by 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.

180
181

2 THE PAN-CANADIAN TRUST FRAMEWORK

2.1 Overview

2.1.1 Background

The identity management ecosystem in Canada is comprised of multiple identity providers relying on authoritative source registries that span provincial/territorial and federal jurisdictions. Consequently, the Canadian ecosystem employs a federated identity model.

The Pan-Canadian Trust Framework (PCTF) is an outcome of the Pan-Canadian approach for federating identities which is an agreement on the principles and standards to be used when developing identity solutions.[3] This approach, embodied in the PCTF, is intended to facilitate the transition to a digital ecosystem which will enable transformative digital service delivery solutions for citizens and residents of Canada.

2.1.2 What is the PCTF?

The PCTF is a model that consists of a set of agreed-on concepts, definitions, processes, conformance criteria, and an assessment approach. It is not a "standard" as such, but is, instead, a framework that relates and applies existing standards, policies, guidelines, and practices, and where such standards and policies do not exist, specifies additional criteria. The role of the PCTF is to complement existing standards and policies such as those concerned with security, privacy, and service delivery.

The PCTF facilitates a common approach between the public sector and the private sector. Use of the PCTF ensures alignment, interoperability, and confidence of digital identity solutions that are intended to work across organizational, sectoral, and jurisdictional boundaries. In addition, the PCTF supplements existing legislation, regulations, and policies.

The PCTF supports the acceptance and mutual recognition of:

- Digital identities of entities such as persons and organizations; and
- Digital relationships between entities.

The PCTF defines a set of discrete process patterns (called atomic processes) that can be mapped to business processes. This mapping makes possible a structured assessment and evaluation of a digital identity solution and identifies any dependencies on external organizations and providers.

[3] See: *Guideline on Identity Assurance* [TBS d., 2017].

The PCTF is technology-agnostic and is defined in a way that encourages innovation and participation in the digital ecosystem. It allows for the interoperability of different platforms, services, architectures, and technologies. Furthermore, the PCTF is designed to take into consideration international digital identity frameworks, such as:

- The Electronic Identification, Authentication, and Trust Services (eIDAS);
- The Financial Action Task Force (FATF); and
- The United Nations Commission on International Trade Law (UNCITRAL).

Finally, it should be noted that the Public Sector Profile of the PCTF, in itself, is not a *governance* framework. Instead, it is a tool to help assess a digital identity program or service.

2.1.3 Scope of the PCTF

Currently, the scope of the Pan-Canadian Trust Framework is:

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

2.2 The PCTF Model

The PCTF Model, as shown in Figure 1, is a high-level overview of the PCTF in diagram form.

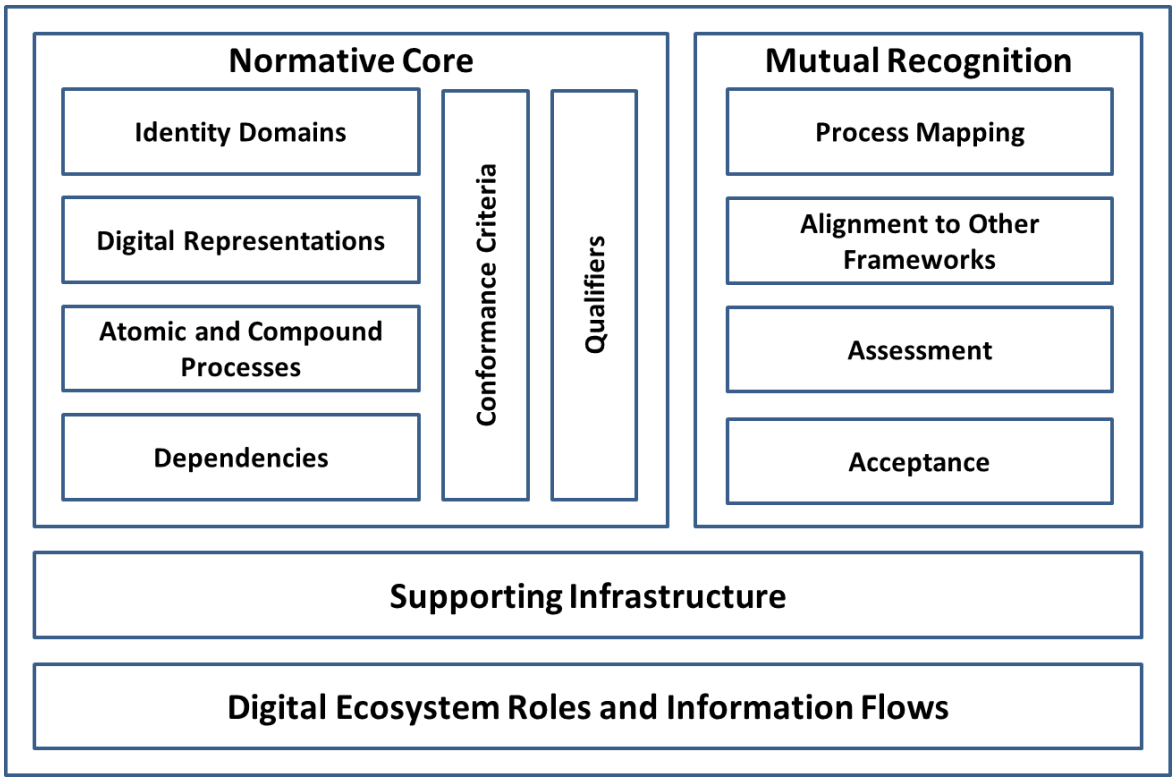

Figure 1: The Pan-Canadian Trust Framework Model

The PCTF model consists of four main components:

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

All items in the "Normative Core" component are prescriptive. The section on the "Mutual Recognition" component describes a recommended methodology but it is not mandatory that the methodology be followed. The sections on the “Supporting Infrastructure” and "Digital Ecosystem Roles and Information Flows" components are descriptive only and not prescriptive.

The four components of the PCTF are described in more detail in the subsequent four sections of this document (Sections 2.3 to 2.6 inclusive).

2.3 Normative Core

2.3.1 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, naturalized citizenship, death, organization legal name registration, organization legal name change, or bankruptcy).
- A **Contextual Identity** is an identity that is used for a specific purpose within a specific identity context[4] (e.g., banking, business permits, health services, drivers licensing, or social media). Depending on the identity context, a contextual identity may be tied to a foundational identity (e.g., a drivers licence) or may not be tied to a foundational identity (e.g., a social media profile).

The establishment and maintenance of foundational identities is the exclusive domain of the public sector; specifically:

- The Vital Statistics Organizations (VSOs) of the Provinces and Territories;
- The Business Registries of the Provinces and Territories;
- Immigration, Refugees, and Citizenship Canada (IRCC); and
- The Federal Corporate Registry of Corporations Canada.

The establishment and maintenance of contextual identities is the domain of both the public and private sectors.

2.3.2 Digital Representations

A digital representation is an electronic representation of an entity or an electronic representation of the relationship between two entities. Digital representations are intended to model real-world actors, such as persons, organizations, and devices.

[4] 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.

Currently, the PCTF recognizes two types of digital representations:

- **Digital Identity**: An electronic representation of an entity, used exclusively by that same entity, to access valued services and to carry out transactions with trust and confidence.
- **Digital Relationship**: An electronic representation of the relationship of one entity to another entity.

A digital representation is the final output of a set of processes and therefore can be conceptualized as a set of state transitions (see Section 2.3.3).

As the PCTF evolves these digital representations will be extended to include other types of entities such as digital assets and smart contracts. It is also anticipated that in the future the PCTF will be used to facilitate the mutual recognition of digital representations between countries.

2.3.3 Atomic and Compound Processes

The PCTF defines a set of atomic processes that can be separately assessed and certified to interoperate with one another in a digital ecosystem. An atomic process is a set of logically related activities that results in a state transition[5]. The PCTF recognizes that in practice a business process is often a collection of atomic processes that results in a set of state transitions. These collections of atomic processes are referred to as compound processes.

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

It should be noted that two atomic processes -- *Identity Information Determination* and *Identity Evidence Determination* – are carried out only once for a program/service.

2.3.3.1 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 by other atomic processes. Figure 2 illustrates the atomic process model.

[5] A state transition is the transformation of an object input state to an output state.

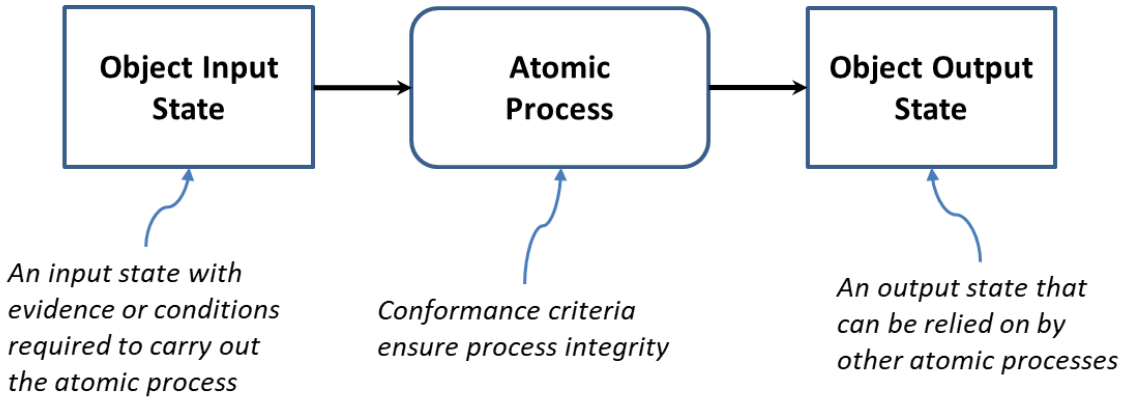

Figure 2: Atomic Process Model

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 party responsible for carrying out the atomic process must ensure that the identifier assigned to the person or organization is unique for a specified population.

The atomic processes are detailed in Section 2.7.

Figure 3 illustrates some model diagrams of three atomic processes.

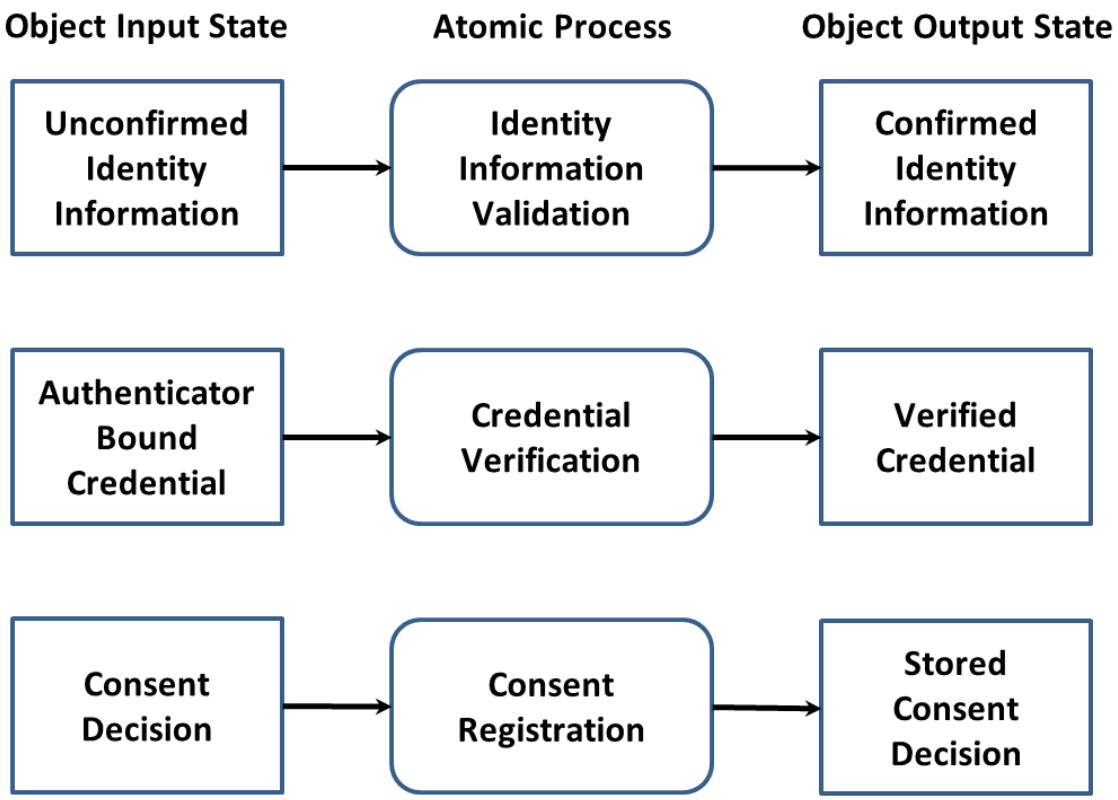

Figure 3: Examples of Atomic Processes (Modeled)

2.3.3.2 Compound Processes

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

For example, a business process that one party refers to as *Identity Confirmation* may in fact turn out to be a compound process consisting of 5 atomic processes as shown in Figure 4.

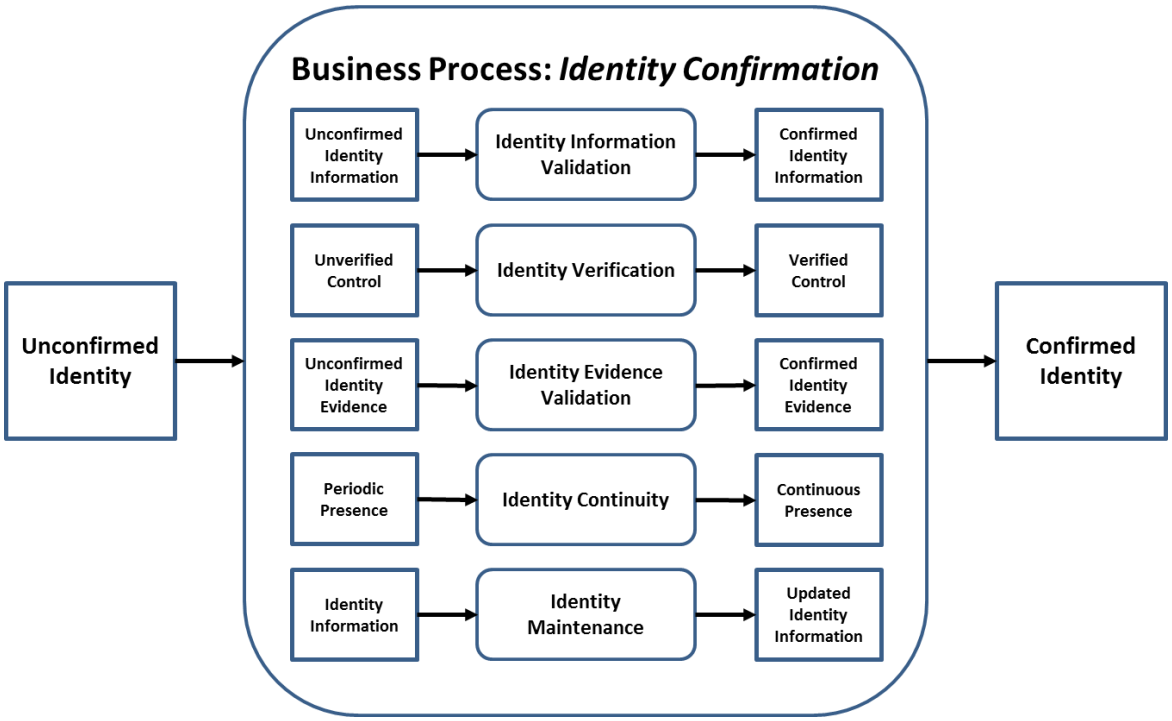

Figure 4: Example of a Compound Process (Modeled)

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

2.3.4 Dependencies

The PCTF model recognizes two types of dependencies. The first type is those dependencies that exist between atomic processes. Although each atomic process is functionally discrete, to produce an acceptable output an atomic process may require the successful prior execution of another atomic process. For example, although *Identity Establishment* of 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. This type of dependency is specified in the conformance criteria (see Section 2.3.5).

The second type is dependencies on external organizations for the provision of atomic process outputs (e.g., a commercial service provider or a credential authentication service). This type of dependency is identified and noted in the assessment process (see Section 2.4.3).

2.3.5 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.

The conformance criteria are maintained in a separate document. Currently, the conformance criteria are consolidated in an assessment worksheet. In future versions the conformance criteria may be embedded in an automated assessment tool.

2.3.6 Qualifiers

Qualifiers may be applied to conformance criteria. Qualifiers are intended to map similar or same conformance criteria from different trust frameworks to jurisdictional policy or regulatory requirements. For example, PCTF Level 1 conformance criteria for the *Identity Verification* atomic process can be mapped to Identity Assurance Level 1 as defined in the *Standard on Identity and Credential Assurance* issued by the Treasury Board of the Government of Canada.

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). Consult the assessment worksheet for examples of how qualifiers are used for assessment and how they may be mapped to other frameworks.

Jurisdictions may wish to use the qualifiers that are already defined in the PCTF. They may also define new qualifiers to reflect their specific requirements and add new conformance criteria if required. New qualifiers may be incorporated back into the normative core component of the PCTF; however, these changes should be subject to a formal governance process or change management process. It should also be noted that if new qualifiers and conformance criteria are introduced into the PCTF, these will need to be mapped to and vetted against the existing conformance criteria. See Section 2.8 for more information on qualifiers.

2.4 Mutual Recognition

Mutual recognition is an agreement wherein two or more parties agree to recognize the results of a conformance assessment. Depending on the context, the mutual recognition may be formalized through the issuance of a letter of acceptance or be part of a broader agreement.

Prior to commencing the PCTF mutual recognition process, it is recommended that a planning and engagement process be undertaken with the key participants in order to develop a formalized work arrangement.

At this time, the mutual recognition process is still in its early stages. The following sections outline mutual recognition at a high level. Detailed guidance will follow in subsequent deliverables.

2.4.1 Process Mapping

Process mapping consists of the set of activities to map program activities, business processes, and technical capabilities to the atomic processes defined in the PCTF.

In most cases, this mapping is applied to an existing program currently in operation. The table below illustrates some examples of mapping to existing business processes.

Atomic Process	Existing Business Process Examples
Identity Resolution	A service enrolment process that attempts to uniquely identify a person based on the person's name and date of birth A business registry process that attempts to uniquely identify an organization based on the organization's legal name, date of creation, address, and identification number/name on an authoritative record
Identity Establishment	A birth registration process that creates an authoritative birth record A business registry process that create an authoritative business record
Identity Information Validation	A driver's license application process that confirms identity information as presented on physical documents or by means of an electronic validation service A cannabis licensing process that confirms identity information as presented about a business by means of an electronic validation with the applicable business registry
Identity	Asking questions of the person presenting the identity information –

Atomic Process	Existing Business Process Examples
Verification	the answers to which (in theory, at least) only they and the interrogator would know (e.g., financial information, credit history, shared secret, mailed-out access code, password, personal identification number, assigned identifier) A passport application process that compares biological characteristics recorded on a document (e.g., facial photograph, eye colour, height) to ensure it is the right applicant Performing an on-site audit of a business
Identity Maintenance	An identity information notification service An identity information retrieval service
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 credential

2.4.2 Alignment to Other Frameworks

Alignment of processes, systems, and solutions assists in mutual recognition across an international context where multiple frameworks may be in use.

For example, someone who accesses Canadian digital services may also need to access digital services in other countries. Recognizing this evolution toward the international context, the PCTF is being designed to be applied in conjunction with established and emerging global frameworks, such as:

- The Electronic Identification, Authentication, and Trust Services (eIDAS)
- The Financial Action Task Force (FATF) – *Guidance on Digital Identity*
- The United Nations Commission on International Trade Law (UNCITRAL) – *Draft Provisions on the Cross-border Recognition of Identity Management and Trust Services*

International mutual recognition is still in its early phases. Consideration should be given to aligning to these frameworks before commencing the assessment process.

2.4.3 Assessment

The PCTF defines a normative set of atomic processes and accompanying conformance criteria[6]. Once the existing business processes have been mapped to the atomic processes, they can be assessed and a determination made against each of the related atomic process conformance criteria.

A detailed assessment worksheet has been developed to assist in the PCTF assessment process. This worksheet consolidates the atomic processes and accompanying conformance criteria into a single spreadsheet to aid in the mapping of existing business processes and assist the assessment team in cross-referencing data for assessment analysis. The conformance criteria are also mapped to qualifiers to assist in the selection of the conformance criteria that are applicable to the assessment process.

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

It should be noted, that by design, the PCTF does not assume that a single provider is solely responsible for all of the atomic processes. Therefore, several bodies might be involved in the PCTF assessment process, focusing on different atomic processes, or different aspects (e.g., security, privacy, service delivery). Consideration must be given as to how to coordinate several bodies that might need to work together to yield an overall PCTF assessment. The organization being assessed is accountable for all parties within the scope of the assessment. The organization may decide that this is not feasible, nonetheless the organization remains accountable. Such cases will be noted in the 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.

2.4.4 Acceptance

Acceptance is the process of formally approving the outcome of the assessment process. The acceptance process is dependent on governance and takes into account the applicable mandates, legislation, regulations, and policies.

Eventually, the PCTF acceptance process may include standard processes defined by the International Standards Organization (ISO)[7] as follows:

[6] The conformance criteria are maintained in a separate document.

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

- **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.

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

2.5 Supporting Infrastructure

The Supporting Infrastructure is the set of operational and technical policies, rules, and standards that serve as the primary enablers of a digital ecosystem. The various elements of the Supporting Infrastructure have established rules that are outside the scope of the PCTF. The PCTF does not make recommendations in respect to the composition of the Supporting Infrastructure.

Figure 5 illustrates some elements (with examples) of what could constitute a Supporting Infrastructure.

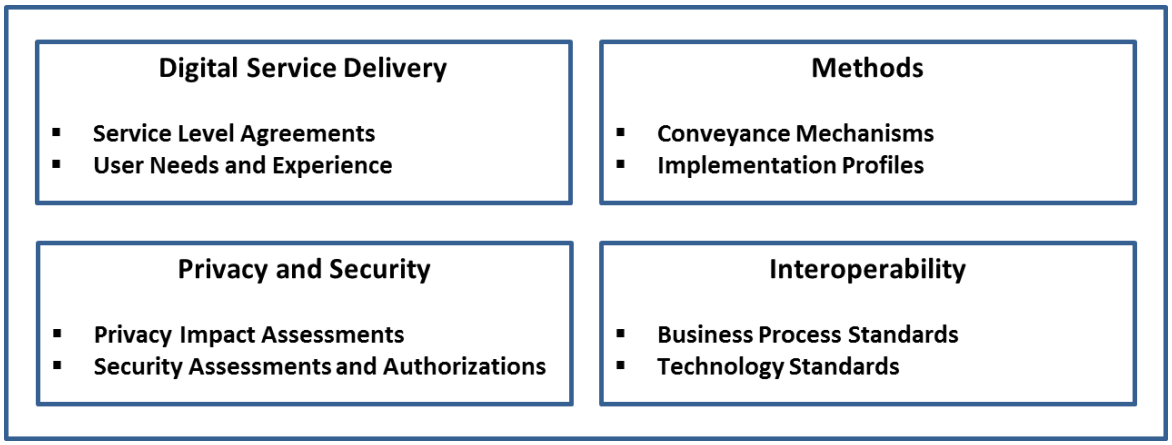

Figure 5: Supporting Infrastructure

The following sections provide details on two elements of the Supporting Infrastructure that can assist in relating legacy implementations to newer technologies and standards.

2.5.1 Methods

Methods encompass the sets of rules that govern such things as data models, communications protocols, cryptographic algorithms, databases, distributed ledgers, verifiable data registries, and similar schemes; and combinations of these. Methods also include systems that are isolated or have intermittent connectivity. Within the context of the digital ecosystem, Methods enable actors to interact directly or indirectly with one another without either party being bound to a particular solution or technology.

2.5.2 Conveyance Mechanisms

Conveyance mechanisms are the various methods by which the output of one atomic process is made available for use as the input to another atomic process. As can be seen in Figure 6, the conveyance mechanisms are situated between the parties producing and consuming the output states of atomic processes.

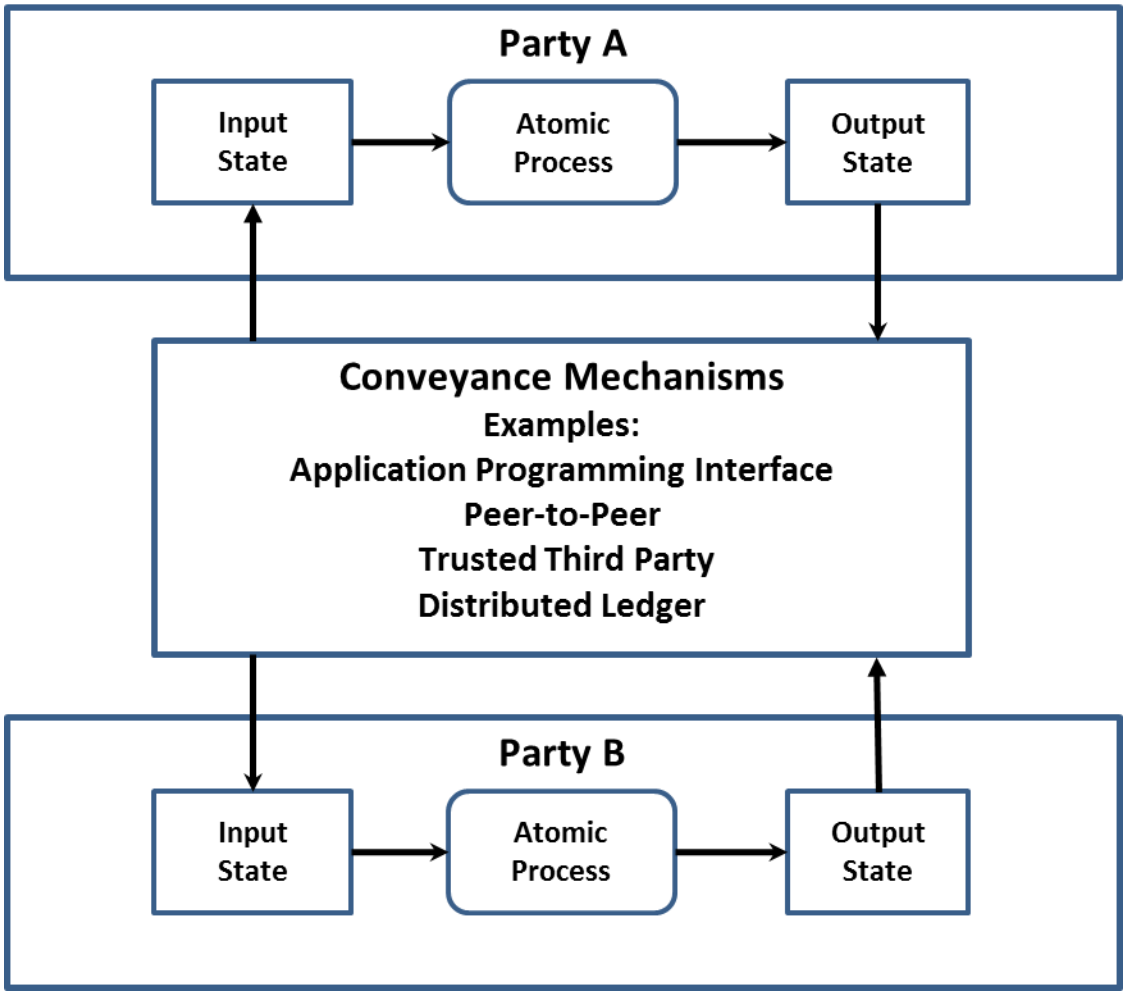

Figure 6: Conveying Output States between Parties

The PCTF does not constrain the possibility of several competing providers and it is anticipated that many providers will coexist to serve the conveyance mechanism needs of different communities across the public and private sector.

2.6 Digital Ecosystem Roles and Information Flows

Figure 7 illustrates a conceptual model of the digital ecosystem roles and information flows. (Note that "Methods" in the diagram is discussed in Section 2.5.1.)

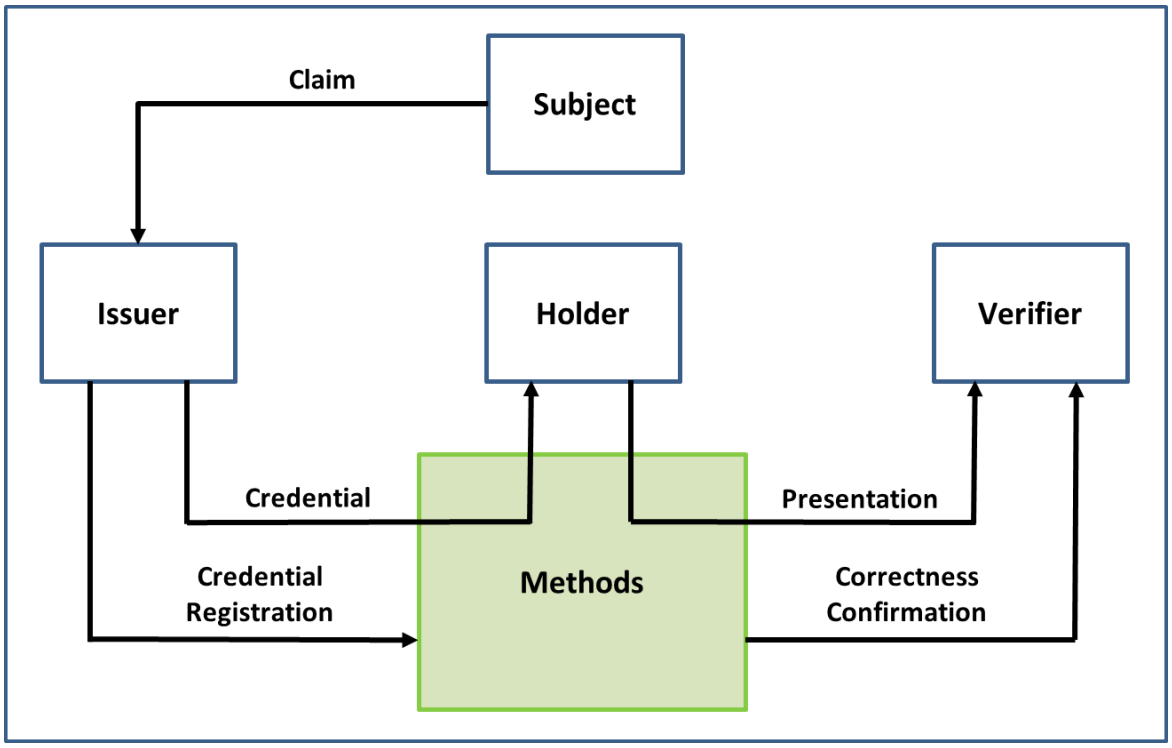

Figure 7: Digital Ecosystem Roles and Information Flows

2.6.1 Roles

The model consists of four roles:

1. **Subject:** An entity[8] about which ***Claims*** are asserted by an ***Issuer***.
2. **Issuer:** An entity that asserts one or more ***Claims*** about one or more ***Subjects***, creates a ***Credential*** from these Claims, and assigns the Credential to a ***Holder***.

[8] An entity is defined as a thing with a distinct and independent existence such as a person, organization, or device that can be subject to legislation, policy, or regulations within a context, and which may have certain rights, duties, and obligations. An entity can perform one or more roles in the digital ecosystem.

3. **Holder:** An entity that controls one or more ***Credentials*** from which a ***Presentation*** can be expressed to a ***Verifier***. A Holder is usually, but not always, the ***Subject*** of a Credential[9].
4. **Verifier**: An entity that accepts a ***Presentation*** from a ***Holder*** for the purposes of delivering services or administering programs.

The digital ecosystem roles are carried out by many different entities that perform specific roles under a variety of labels. These specific roles can be categorized into the digital ecosystem roles as shown in the following table.

Role	Examples
Issuer	Authoritative Party, Identity Assurance Provider, Identity Proofing Service Provider, Identity Provider, Credential Assurance Provider, Credential Service Provider, Credential Provider, Authenticator Provider, Digital Identity Provider, Delegated Service Provider
Subject	Person, Organization, Device
Holder	Digital Identity Owner, Card Holder
Verifier	Relying Party, Credential Verification Service Provider, Credential Authentication Service Provider, Authentication Service Provider, Digital Identity Consumer, Delegated Service Provider

Given the variety of business, service, and technology models that exist within the digital ecosystem, roles may be performed by multiple different actors in a given context, or one actor may perform several roles (e.g., an actor may be both a relying party and a credential provider).

In addition to the four roles outlined above, digital ecosystem actors include Supporting Infrastructure providers such as Network Operators.

[9] Examples of where the Holder is not the Subject of a Credential would be a parent (the holder) holding the birth certificate (the credential) of their child (the subject) or a restaurant owner (the holder) holding a permit to operate (the credential) of a business (the subject).

2.6.2 Information Flows

The model also consists of five information flows:

1. **Claim:** A statement about a ***Subject***.
2. **Credential:** A set of one or more ***Claims*** asserted about one or more ***Subjects***[10].
3. **Presentation:** Information derived from one or more ***Credentials***. The data in a Presentation is often about the same ***Subject***, but the Credentials might have been issued by different ***Issuers***.
4. **Credential Registration:** An indication[11] of the existence of a credential.
5. **Correctness Confirmation**[12]**:** An indication of the correctness of the ***Presentation*** itself and the correctness of the information associated with the ***Presentation***.

[10] An example of a credential having more than one subject is a marriage certificate.

[11] The indication may be a credential schema or the credential itself.

[12] Correctness confirmation is often achieved by connecting a Verifier to an Issuer through a peer-to-peer system or an intermediary system.

580

581 2.7 Atomic Processes in Detail

582 2.7.1 Identity Information Determination

Process Description	Identity Information Determination is the process of determining the identity context[13], the identity information requirements[14], and the identifier[15].
Input State	**No Determination Made**: The identity context, the identity information requirements, and the identifier have not been determined
Output State	**Determination Made**: The identity context, the identity information requirements, and the identifier have been determined

583 2.7.2 Identity Evidence Determination

Process Description	Identity Evidence Determination is the process of determining the acceptable evidence of identity (whether physical or electronic).
Input State	**No Determination Made**: The acceptable evidence of identity has not been determined
Output State	**Determination Made**: The acceptable evidence of identity has been determined

584 2.7.3 Identity Resolution

Process Description	Identity Resolution is the process of establishing the uniqueness of a Subject 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	**Identity Information**: The identity information may or may not be unique to one and only one Subject
Output State	**Unique Identity Information**: The identity information is unique to one and only one Subject

[13] See Section 4.3 for more information.

[14] See Section 4.4 for more information.

[15] See Section 4.4.1 for more information.

585 ### 2.7.4 Identity Establishment

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

586 ### 2.7.5 Identity Information Validation

Process Description	Identity Information Validation is the process of confirming the accuracy of identity information about a Subject as established by the Issuer.
Input State	**Unconfirmed Identity Information**: The identity information has not been confirmed with the Issuer
Output State	**Confirmed Identity Information**: The identity information has been confirmed with the Issuer

587 ### 2.7.6 Identity Verification

Process Description	Identity Verification is the process of confirming that the identity information is under the control of the Subject. It should be noted that this process may use personal information or organizational information that is not related to identity.
Input State	**Unverified Control**: The identity information has not been verified as being under the control of the Subject
Output State	**Verified Control**: The identity information has been verified as being under the control of the Subject

588 ### 2.7.7 Identity Evidence Validation

Process Description	Identity Evidence Validation is the process of confirming that the evidence of identity presented (whether physical or electronic) is acceptable.
Input State	**Unconfirmed Identity Evidence**: The evidence of identity has not been confirmed as being acceptable
Output State	**Confirmed Identity Evidence**: The evidence of identity has been confirmed as being acceptable

2.7.8 Identity Continuity

Process Description	Identity Continuity is the process of dynamically confirming that the Subject 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	**Periodic Presence**: The identity exists sporadically and often only in association with a vital event or a business event (e.g., birth, death, bankruptcy)
Output State	**Continuous Presence**: The identity exists continuously over time in association with many transactions

2.7.9 Identity Maintenance

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

2.7.10 Identity Linking

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

2.7.11 Credential-Identity Binding

Process Description	Credential-Identity Binding is the process of asserting one or more Claims about one or more Subjects.
Input State	**No Claim**: No claim exists
Output State	**Asserted Claim**: One or more asserted claims has been associated with one or more Subjects

2.7.12 Credential Issuance

Process Description	Credential Issuance is the process of creating a Credential from a set of Claims and assigning the Credential to a Holder.
Input State	**Asserted Claim**: One or more asserted claims has been associated with one or more Subjects
Output State	**Issued Credential**: A credential has been assigned to a Holder

2.7.13 Credential-Authenticator Binding

Process Description	Credential-Authenticator Binding is the process of associating a credential issued to a Holder with one or more authenticators. This process also includes authenticator life-cycle activities such as suspending authenticators (caused by a forgotten password or a lockout due to successive failed authentications, inactivity, or suspicious activity), removing authenticators, binding new authenticators, and updating authenticators (e.g., changing a password, updating security questions and answers, having a new facial photo taken).
Input State	**Issued Credential**: A credential has been assigned to a Holder
Output State	**Authenticator Bound Credential**: An issued credential has been associated with one or more authenticators

2.7.14 Credential Validation

Process Description	Credential Validation is the process of verifying that the issued credential is valid (e.g., not tampered with, corrupted, modified, suspended, or revoked). The validity of the issued credential can be used to generate a level of assurance.
Input State	**Authenticator Bound Credential**: An issued credential has been associated with one or more authenticators
Output State	**Validated Credential**: The issued credential is valid

598 ### 2.7.15 Credential Verification

Process Description	Credential Verification is the process of verifying that a Holder has control over an issued credential. Control of an issued credential is verified by means one or more authenticators. The degree of control over the issued credential can be used to generate a level of assurance.
Input State	**Authenticator Bound Credential**: An issued credential has been associated with one or more authenticators
Output State	**Verified Credential**: The Holder has proven control of the issued credential

599 ### 2.7.16 Credential Maintenance

Process Description	Credential Maintenance is the process of updating the credential attributes (e.g., expiry date, scope of service, permissions) of an issued credential.
Input State	**Issued Credential**: A credential has been assigned to a Holder
Output State	**Updated Issued Credential**: The issued credential has been updated

600 ### 2.7.17 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 credential has been assigned to a Holder
Output State	**Suspended Credential**: The Holder is not able to use the credential

601 ### 2.7.18 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 Holder is not able to use the credential
Output State	**Updated Issued Credential**: The issued credential has been updated

602

603 ### 2.7.19 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 credential has been assigned to a Holder
Output State	**Revoked Credential**: The Holder is not able to use the credential

604

605 ### 2.7.20 Notice Formulation

Process Description	Notice Formulation 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 (as known at the time of presentation); 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. This process should be carried out in accordance with any requirements of jurisdictional legislation and regulation.
Input State	**No Notice Statement**: No notice statement exists
Output State	**Notice Statement**: A notice statement exists

606 ### 2.7.21 Notice Presentation

Process Description	Notice Presentation is the process of presenting a notice statement to a person.
Input State	**Notice Statement**: A notice statement exists
Output State	**Presented Notice Statement**: A notice statement has been presented to a person

607 ### 2.7.22 Consent Request

Process Description	Consent Request is the process of asking a person to agree to provide consent (“Yes”) or decline to provide consent (“No”) based on the contents of a presented notice statement, resulting in either a “yes” or “no” consent decision.
Input State	**Presented Notice Statement**: A notice statement has been presented to a person
Output State	**Consent Decision**: A consent decision exists

608

609 ### 2.7.23 Consent Registration

Process Description	Consent Registration is the process of persisting a notice statement and the person's related consent decision, to storage. In addition, information about the person, 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

610 ### 2.7.24 Consent Review

Process Description	Consent Review is the process of making the details of a stored consent decision visible to the person who provided the consent.
Input State	**Stored Consent Decision**: A stored consent decision exists
Output State	**Stored Consent Decision**: A stored consent decision exists

611 ### 2.7.25 Consent Renewal

Process Description	Consent Renewal 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	**Updated Consent Decision**: A stored consent decision has been updated

612 ### 2.7.26 Consent Expiration

Process Description	Consent Expiration 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	**Updated Consent Decision**: A stored consent decision has been updated

613

2.7.27 Consent Revocation

Process Description	Consent Revocation is the process of suspending the validity of a "yes" consent decision as a result of an explicit withdrawal of consent by the person (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	**Updated Consent Decision**: A stored consent decision has been updated

2.7.28 Signature Creation

Process Description	Signature Creation is the process of creating a signature.
Input State	**No Signature**: No signature exists
Output State	**Signature**: A signature exists

2.7.29 Signature Checking

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

621
622
623

2.8 Qualifiers in Detail

2.8.1 Identity Domain Qualifiers

To reflect the shared responsibility of identity across jurisdictions within the Pan-Canadian context, two identity domain qualifiers have been defined:

- **Foundational Identity Domain**: Conformance criteria that are tied to a specific foundational event (e.g., birth, person legal name change, immigration, legal residency, naturalized citizenship, death, organization legal name registration, organization legal name change, or bankruptcy). Foundational identities are the exclusive domain of the public sector (specifically, the Vital Statistics Organizations [VSOs] and Business Registries of the Provinces and Territories; Immigration, Refugees, and Citizenship Canada [IRCC]; and the Federal Corporate Registry of Corporations Canada).
- **Contextual Identity Domain**: Conformance criteria that are specific to an identity context (e.g., banking, business permits, health services, drivers licensing, or social media). Depending on the identity context, a contextual identity may be tied to a foundational identity (e.g., a drivers licence) or may not be tied to a foundational identity (e.g., a social media profile). Contextual identities are the domain of both the public and private sectors.

2.8.2 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.

2.8.3 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*** defined in its annexed *Secure Electronic Signature [SES] Regulations*). Secure electronic signatures may be used as qualifiers.

2.8.4 Other Trust Frameworks 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:

- **Low**: How degree of confidence.
- **Substantial**: Substantial degree of confidence.
- **High**: High degree of confidence.

Qualifiers may be based on levels of assurance defined in the 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.

3 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 a person, does not reveal the person's identity. A credential may contain identity attributes but still be treated as an anonymous credential if the identity attributes are not recognized or used for identity information validation purposes. Anonymous credentials provide persons with a means to prove statements about themselves and their relationships with other persons or organizations while maintaining their anonymity.
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	Confidence that a statement is true.
assurance level	A level of confidence that a statement is true 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 by other atomic processes.
attribute	A property or characteristic associated with an entity. See also "identity attribute".
authentication	See "credential verification".
authenticator	Something that a Holder controls (e.g., a cryptographic module or a password) that is used to prove that the Holder has retained control over an issued credential.
authoritative source	A collection or registry of records maintained by an authority that meets established criteria.

Term	Definition
biological or behavioural characteristic confirmation	An identity verification method that uses biological (anatomical and physiological) characteristics (e.g., face, fingerprints, retinas) or behavioural characteristics (e.g., keyboard stroke timing, gait) to prove that the person presenting the identity information is in control of the identity. Biological or behavioural characteristic confirmation is achieved by means of the challenge-response model: the biological or behavioural characteristics recorded on a document or in a data store are compared to the person presenting the identity information.
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.
claim	A statement about a Subject.
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 employees and contractors.
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.
consent expiration	The process of suspending the validity of a “yes” consent decision as a result of exceeding an expiration date limit.

Term	Definition
consent registration	The process of persisting a notice statement and the person's related consent decision, to storage. In addition, information about the person, 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.
consent renewal	The process of extending the validity of a "yes" consent decision by means of increasing an expiration date limit.
consent request	The process of asking a person to agree to provide consent ("Yes") or decline to provide consent ("No") based on the contents of a presented notice statement, resulting in either a "yes" or "no" consent decision.
consent review	The process of making the details of a stored consent decision visible to the person who provided the consent.
consent revocation	The process of suspending the validity of a "yes" consent decision as a result of an explicit withdrawal of consent by the person (i.e., a "yes" consent decision is converted into a "no" consent decision).
contextual identity	An identity that is used for a specific purpose within a specific identity context (e.g., banking, business permits, health services, drivers licensing, or social media). Depending on the identity context, a contextual identity may be tied to a foundational identity (e.g., a drivers licence) or may not be tied to a foundational identity (e.g., a social media profile).
correctness confirmation	An indication of the correctness of the Presentation itself and the correctness of the information associated with the Presentation.
credential	A set of one or more Claims asserted about one or more Subjects.
credential assurance	Confidence that a Holder has maintained control over an issued credential and that the issued credential is valid.

Term	Definition
credential assurance level	The level of confidence that a Holder has maintained control over an issued credential and that the issued credential is valid.
credential-authenticator binding	The process of associating a credential issued to a Holder with one or more authenticators. This process also includes authenticator life-cycle activities such as suspending authenticators (caused by a forgotten password or a lockout due to successive failed authentications, inactivity, or suspicious activity), removing authenticators, binding new authenticators, and updating authenticators (e.g., changing a password, updating security questions and answers, having a new facial photo taken).
credential-identity binding	The process of asserting one or more claims about one or more Subjects.
credential issuance	The process of creating a credential from a set of claims and assigning the credential to a Holder.
credential maintenance	The process of updating the credential attributes (e.g., expiry date, scope of service, permissions) of an issued credential.
credential recovery	The process of transforming a suspended credential back to a usable state (i.e., an issued credential).
credential registration	An indication of the existence of a credential.
credential revocation	The process of ensuring that an issued credential is permanently flagged as unusable.
credential suspension	The process of transforming an issued credential into a suspended credential by flagging the issued credential as temporarily unusable.
credential validation	The process of verifying that the issued credential is valid (e.g., not tampered with, corrupted, modified, suspended, or revoked). The validity of the issued credential can be used to generate a level of assurance.

Term	Definition
credential verification	The process of verifying that a Holder has control over an issued credential. Control of an issued credential is verified by means one or more authenticators. The degree of control over the issued credential can be used to generate a level of assurance.
device	A machine, specifically a piece of electronic equipment.
digital ecosystem	A collection of various tools and systems, and the actors who create, interact with, use, and remake them.
digital identity	An electronic representation of an entity, used exclusively by that same entity, to access valued services and to carry out transactions with trust and confidence.
digital relationship	An electronic representation of the relationship of one entity to another entity.
digital representation	An electronic representation of an entity or an electronic representation of the relationship between two entities.
eIDAS	Electronic Identification, Authentication, and Trust Services eIDAS is a European Union regulation that oversees electronic identification and trust services for electronic transactions in the European Union's internal market. It regulates electronic signatures, electronic transactions, involved bodies, and their embedding processes to provide a safe way for users to conduct business online such as electronic funds transfer or transactions with public services.
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.
entity	A thing with a distinct and independent existence such as a person, organization, or device that can be subject to legislation, policy, or regulations within a context, and which may have certain rights, duties, and obligations. An entity can perform one or more roles in the digital ecosystem.
evidence of contextual	Evidence of identity that corroborates the evidence of

Term	Definition
identity	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; 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 records of licences to carry on logging or mining activities, or to cultivate cannabis; and registrations of charitable status.
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 an entity's identity. There are two categories of evidence of identity: foundational and contextual. See "evidence of foundational identity" and "evidence of contextual identity".

Term	Definition
FATF	Financial Action Task Force FATF is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada FINTRAC is Canada's financial intelligence unit. Its mandate is to facilitate the detection, prevention, and deterrence of money laundering and the financing of terrorist activities.
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 business registry record, federal corporate registry record).
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 provincial and territorial VSO registries and 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 provincial and territorial business registries and Corporations Canada [federal]).
foundational event	A foundational event is either a business event or a vital event. Business events and vital events are significant discrete episodes that occur in the life spans of businesses and persons, respectively. By law both business events and vital events must be recorded with a government entity and are subject to legislation and

Term	Definition
	regulation. See “business event” and “vital event”.
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	Refers to a social identity, such as man, woman, non-binary, or two-spirit.
holder	An entity that controls one or more Credentials from which a Presentation can be expressed to a Verifier. A Holder is usually, but not always, the Subject of a Credential.
identifier	The set of identity attributes used to uniquely distinguish a particular person, organization, or device within a population.
identity	A reference or designation used to uniquely distinguish a particular person, organization, or device. There are two types of identity: foundational and contextual. See “foundational identity” and “contextual identity”.
identity assurance	Confidence 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.
identity attribute	A property or characteristic associated with an identifiable person, organization, or device (also known as “identity data element”).
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 continuity	The process of dynamically confirming that the Subject has a continuous existence over time (i.e., “genuine

Term	Definition
	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 data element	See "identity attribute".
identity establishment	The process of creating a record of identity of a Subject within a program/service population that may be relied on by others for subsequent programs, services, and activities.
identity evidence determination	The process of determining the acceptable evidence of identity (whether physical or electronic).
identity evidence validation	The process of confirming that the evidence of identity presented (whether physical or electronic) is acceptable.
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.
identity information determination	The process of determining the identity context, the identity information requirements, and the identifier.
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 Subject as established by the Issuer.

Term	Definition
identity linking	The process of mapping two or more identifiers to the same Subject.
identity maintenance	The process of ensuring that a Subject's identity information is accurate, complete, and up-to-date.
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 resolution	The process of establishing the uniqueness of a Subject within a program/service population through the use of identity information.
identity scheme	See "identity model".
identity verification	The process of confirming that the identity information is under the control of the Subject. It should be noted that this process may use personal information or organizational information that is not related to identity.
issuer	An entity that asserts one or more Claims about one or more Subjects, creates a Credential from these Claims, and assigns the Credential to a Holder.
knowledge-based confirmation	An identity verification method that uses personal or organizational information or shared secrets to prove that the person or organization presenting the identity information is in control of the identity. Knowledge-based confirmation is achieved by means of the challenge-response model: the person or organization presenting the identity information is asked questions, the answers to which (in theory, at least) only they and the interrogator would know (e.g., financial information, credit history, shared secret, cryptographic key, mailed-out access code, password, personal identification number, assigned identifier).

Term	Definition
legal name	See “foundation name”, “primary name”.
legal presence	Lawful entitlement to be or reside in Canada.
methods	The sets of rules that govern such things as data models, communications protocols, cryptographic algorithms, distributed ledgers, databases, and similar schemes; and combinations of these.
NIST	National Institute of Standards and Technology NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology.
notice formulation	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 (as known at the time of presentation); 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. This process should be carried out in accordance with any requirements of jurisdictional legislation and regulation.
notice presentation	The process of presenting a notice statement to a person.
organization	A legal entity that is not a human being (in legal terms a “juridical person”).
organizational information	Information about an identifiable organization.
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.

Term	Definition
physical possession confirmation	An identity verification method that requires physical possession or presentation of evidence to prove that the person or organization presenting the identity information is in control of the identity.
preferred name	The name by which a person prefers to be informally addressed.
presentation	Information derived from one or more Credentials. The data in a Presentation is often about the same Subject, but the Credentials might have been issued by different Issuers.
primary name	The name that a person or organization uses for formal and legal purposes (also known as “legal name”). See also “foundation name”.
sex	Refers to biological characteristics, such as male, female, or intersex.
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.
signature checking	The process of confirming that the signature is valid.
signature creation	The process of creating a signature.
subject	An entity about which Claims are asserted by an Issuer.
supporting infrastructure	The set of operational and technical policies, rules, and standards that serve as the primary enablers of a digital ecosystem.
trust framework	A set of agreed on principles, definitions, standards, specifications, conformance criteria, and assessment approach.

Term	Definition
trusted referee confirmation	An identity verification method that relies on a trusted referee to prove that the person or organization presenting the identity information is in control of the identity. The type of trusted referee and their acceptability is determined by program-specific criteria. Examples of trusted referees include guarantors, notaries, accountants, and certified agents.
UNCITRAL	United Nations Commission on International Trade Law UNCITRAL's mandate is to promote the progressive harmonization and unification of international trade law through conventions, model laws, and other instruments that address key areas of commerce, from dispute resolution to the procurement and sale of goods.
verifier	An entity that accepts a Presentation from a Holder for the purposes of delivering services or administering programs.
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, stillbirth, adoption, legitimation, recognition of parenthood, immigration, legal residency, naturalized citizenship, name change, marriage, annulment of marriage, legal separation, divorce, and death.

679

680

681

682

683

684

4 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 d., 2015].

4.1 Identity

4.1.1 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[16]

4.1.2 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[17]. 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.

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

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

4.2 Defining the Population

In the Canadian context, the universe of persons is defined as all citizens and residents of Canada (including deceased persons) for whom an identity has been established in Canada. The universe of organizations is defined as all organizations registered in Canada (including inactive organizations) for which an identity has been established in Canada. Those persons or organizations that fall within the mandate of a program or service constitute the population of the program or service[18].

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

4.3 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.

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

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, 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 where the shared service delivery context may differ from the program context

4.4 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 for a person include *name* and *date of birth*. Examples of identity attributes for an organization include *legal name* and *date of creation*. 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”). Personal information or organizational information that is collected and used for the specific purpose of administering a program or delivering a service is referred to as *program-specific* personal information or *program-specific* organizational information. Program-specific personal information is usually restricted to the program and constrained by privacy legislation to ensure consistent use for which it was collected (e.g., to determine program eligibility), with a few exceptions.

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[19]. 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.

4.4.1 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 identity 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 and regulation. 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*[20] (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.

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

[20] See the next section.

- **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.

These four factors are not an exhaustive list. Another factor that might be considered is whether the program or service has the legal authority to collect the identity attribute. Yet another factor might be the degree of invasiveness of collecting an identity attribute when other identity attributes might be sufficient for the purpose (e.g., DNA samples shouldn't be collected where name would suffice).

4.4.2 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[21] 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.

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

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 the 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 which may vary between sectors and jurisdictions. For example, the Government of Canada imposes restrictions on the collection, use, retention, disclosure, and disposal of the social insurance number.

4.5 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.

4.6 Ensuring the Accuracy of Identity Information

Identity information must be accurate, complete, and up to date[22]. 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 complete and up to date.

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.

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 two methods by which this can be achieved:

- 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 both.

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.

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

905

5 APPENDIX C: PERSONS AND ORGANIZATIONS

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

5.1 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.

5.2 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.

5.3 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[23] 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.

[23] 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.

5.4 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.

5.5 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

From this table it can be seen that whereas all personal information is subject to privacy and protection guarantees, organizational information is not considered private but some organizational information may be protected by confidentiality agreements.

6 APPENDIX D: IDENTITY AND CREDENTIAL VERIFICATION

This appendix provides some additional background information on the nature of identity verification and credential verification.

6.1 Identity Verification

Identity Verification is the process of confirming that the identity information is under the control of the Subject. It should be noted that this process may use personal information or organizational information that is not related to identity. There are 4 methods used to achieve identity verification:

Knowledge-based confirmation: An identity verification method that uses personal or organizational information or shared secrets to prove that the person or organization presenting the identity information is in control of the identity. Knowledge-based confirmation is achieved by means of the challenge-response model: the person or organization presenting the identity information is asked questions, the answers to which (in theory, at least) only they and the interrogator would know (e.g., financial information, credit history, shared secret, cryptographic key, mailed-out access code, password, personal identification number, assigned identifier).

Biological or behavioural characteristic confirmation: An identity verification method that uses biological (anatomical and physiological) characteristics (e.g., face, fingerprints, retinas) or behavioural characteristics (e.g., keyboard stroke timing, gait) to prove that the person presenting the identity information is in control of the identity. Biological or behavioural characteristic confirmation is achieved by means of the challenge-response model: the biological or behavioural characteristics recorded on a document or in a data store are compared to the person presenting the identity information

Physical possession confirmation: An identity verification method that requires physical possession or presentation of evidence to prove that the person or organization presenting the identity information is in control of the identity.

Trusted referee confirmation: An identity verification method that relies on a trusted referee to prove that the person or organization presenting the identity information is in control of the identity. The type of trusted referee and their acceptability is determined by program-specific criteria. Examples of trusted referees include guarantors, notaries, accountants, and certified agents.

6.2 Credential Verification

Credential Verification is the process of verifying that a Holder has control over an issued credential. Control of an issued credential is verified by means of one or more authenticators. The degree of control over the issued credential and the status of the issued credential (i.e., not tampered with, corrupted, modified, suspended, or revoked) can be used to generate a level of assurance. The Credential Verification process is also used to prove that the Holder is the same entity as the entity in the previous transaction.

The Credential Verification process is dependent on the **Credential-Authenticator Binding** process:

> **Credential-Authenticator Binding**: The process of associating a credential issued to a Holder with one or more authenticators.
>
> An authenticator is something that a Holder controls that is used to prove that the Holder has retained control over an issued credential. There are 3 types of authenticators:
>
> - Something the Holder has (e.g., a cryptographic key or a one-time-password). This is similar to physical possession confirmation used by Identity Verification.
> - Something the Holder knows (i.e., knowledge-based authenticators [KBAs]) (e.g., a password, a response to a challenge question). This is similar to knowledge-based confirmation used by Identity Verification.
> - Something the Holder is or does (e.g., face, fingerprints, retinas, keyboard stroke timing, gait). This is similar to biological or behavioural characteristic confirmation used by Identity Verification.
>
> The Credential-Authenticator Binding process also includes authenticator life-cycle activities such as suspending authenticators (caused by a forgotten password or a lockout due to successive failed authentications, inactivity, or suspicious activity), removing authenticators, binding new authenticators, and updating authenticators (e.g., changing a password, updating security questions and answers, having a new facial photo taken).

7 APPENDIX E: GUIDELINES ON MUTUAL RECOGNITION

At this time, the mutual recognition process is still in its early stages. The following sections outline some guidelines on mutual recognition at a high level. Detailed guidance will follow in subsequent deliverables.

7.1 Planning and Engagement

The planning and engagement step should include the following:

- **Define the Scope of the Assessment**. The scope of the assessment may include one or more parties acting in the roles defined as part of the digital ecosystem. While the primary focus of the assessment is usually a jurisdiction as an "issuer", the assessment may include additional parties who have been delegated specific business functions or roles. The PCTF model may also be used to clarify roles and responsibilities that are relevant to, but not necessarily within the scope of the formal assessment process.
- **Formalize the Team.** Formalize the mutual recognition project team who will be responsible for the process and deliverables. The project team should consist of the assessment team and members from the participating organizations who have detailed operational knowledge of the program.
- **Site Visit.** The assessment team should perform a site visit. The desired outcome is to ensure that the assessment team members can gain direct knowledge of the program and establish close working relationships with the other mutual recognition project team members to facilitate knowledge transfer and shared understanding.
- **Define a Discrete Work Stream**. While the mutual recognition project team may be integrated into a larger project initiative, the mutual recognition process should be maintained as a discrete work stream. However, the work stream should have tight synchronization with the other work streams, such as privacy impact assessments, security assessment and authorization, and technical integration.
- **Engage Legal Counsel Early**. It is recommended that legal counsel of all parties be engaged early in the process. As the assessment process and the ensuing arrangements may be new in relation to existing arrangements, there may be implications for respective authorities and agreements.
- **Engage Privacy and Security Early**. It is recommended that the privacy and security officials of all parties be engaged early in the process since Privacy Impact Assessments and Security Assessments will need to be conducted.

- **Records Management**. Ensure that all evidence received, and assessment documents and working drafts are filed in a proper records management system under the appropriate security categorization. Upon completion of the assessment, all material should be finalized as records for audit purposes.

7.2 Process Mapping

The following are some recommendations for the process mapping step:

- **Define the Scope of the Mapping.** Typically the mapping will be of an established program or business line. The scope of the mapping may include upstream programs such as vital statistics or external commercial service providers. These may be included in the scope of the assessment or identified as *dependencies*.
- **Be Prepared for Terminology Variation.** Many programs under assessment will be well-established and using terminology for their context. The purpose of the mapping process is not to introduce new terminology, but rather to map what exists in name to what needs to be assessed using the PCTF.
- **Work closely with all Team Members.** A large part of the process mapping is a discovery process by the team. While existing documentation may be the primary source of information, interviews with subject matter experts and operational personnel may be required. Workshops may also need to be held to arrive at a common understanding and mapping.
- **Clarify Responsibilities Between Parties.** Similar processes may be carried out or duplicated across the different parties. For example, “enrolment” in a digital identity program, may be the same as or different from a subsequent “enrolment” in a service that has accepted the digital identity. The mapping of the atomic processes can help to clarify what may be a duplicate (i.e., redundant) process to the user, and what may be specifically required for the service.

7.3 Assessment

Assessment requires a judgment call by an impartial expert using the best and most complete information available. At its simplest, the assessment determination may be a simple PASS/FAIL. However, in practice, the assessor may require additional gradations to express concerns made at the time of the determination or to reflect that certain information may be incomplete or unavailable to the assessor.

The following are the assessment determinations that have been developed so far and which may be adjusted over time. It is cautioned that assessment determinations having too many gradations may make the assessment process less transparent.

The current assessment determinations in use 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.

7.4 Acceptance

Upon completion of the assessment process, a *Letter of Acceptance* is issued to the jurisdiction. This letter should:

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

1206
1207

8 APPENDIX F: THEMATIC ISSUES

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

Thematic Issue 1: Digital Relationships

We need to work on expanding our modeling and discussion of digital relationships – currently, there is not much more than a definition.

Thematic Issue 2: The Evolving State of Credentials

We now find ourselves in the middle of some very interesting developments in the areas of digital credentials. There is a sea-change happening in the industry where there is a movement from 'information-sharing' to 'presenting digital proofs'. There is 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 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 3: 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 especially in relation to the public sector. We have incorporated material from the DIACC and we have adjusted this material for public sector considerations, but we feel that much more work needs to be done. In 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 4: 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 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 5: 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 and British Columbia). The PCTF will be supplemented with detailed guidance in a separate document.

Thematic Issue 6: Unregistered Organizations

Currently, the scope of PCTF includes "all organizations registered in Canada (including inactive organizations) for which an identity has been established in Canada". There are also many kinds of *unregistered* organizations operating in Canada such as sole proprietorships, trade unions, co-ops, NGOs, unregistered charities, and trusts. An analysis of these unregistered organizations in relation to the PCTF needs to be undertaken.

Thematic Issue 7: Assessing Outsourced Atomic Processes

Section 2.4.3 states that:

> by design, the PCTF does not assume that a single provider is solely responsible for all of the atomic processes. Therefore, several bodies might be involved in the PCTF assessment process, focusing on different atomic processes, or different aspects (e.g., security, privacy, service delivery). Consideration must be given as to how to coordinate several bodies that might need to work together to yield an overall PCTF assessment. The organization being assessed is accountable for all parties within the scope of the assessment. The organization may decide that this is not feasible, nonetheless the organization remains accountable. Such cases will be noted in the assessment.

The Issuer in this model is the authority ultimately accountable. Although an Issuer may choose to outsource or delegate the responsibility of the *Credential Issuance* atomic process to another body, the accountability remains with the Issuer.

We need to determine how multi-actor assessments will be conducted. It has been suggested that the organization being assessed should have the authority to speak to how well other organizations perform atomic processes on its behalf.

Thematic Issue 8: The *Identity Continuity* Atomic Process

The *Identity Continuity* atomic process is defined as:

> the process of dynamically confirming that the Subject 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.

It has been noted that there are privacy concerns with the notion of "dynamically confirming" the continuous existence of a Subject over time. We need to come up with a more precise and privacy-respecting definition of the *Identity Continuity* atomic process.

Thematic Issue 9: Signature

Appendix A defines *signature* as:

> 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.

We need to explore how the concept of signature is to be applied in the context of the PCTF.

Thematic Issue 10: Foundation Name, Primary Name, Legal Name

Appendix A has definitions for *Foundation Name*, *Primary Name*, and *Legal Name*.

The three terms more or less mean the same thing. We need to pick the preferred term and be consistent in its usage.

Thematic Issue 11: Review of the Appendices

At some point we should undertake a full review of the current appendices. For each appendix, we need to evaluate its utility, applicability, and appropriateness, and determine if it should continue to be included in the PCTF document. Some appendices will remain; some may be moved to a guidelines document; while others might be discarded outright. Some of the appendices that remain may need to be amended.

1308

1309

1310

9 APPENDIX G: BIBLIOGRAPHY

Organizations

1. Canadian Joint Councils (CJC)
    a. Canadian Joint Councils' Digital Identity Priority: Public Policy Recommendations (2018)
2. Communications Security Establishment (CSE)
    a. User Authentication Guidance for Information Technology Systems (2018)
3. Digital Identity and Authentication Council of Canada (DIACC)
    a. Pan-Canadian Trust Framework Model Overview (February 2019)
    b. Notice and Consent Component Overview (April 2019)
    c. Pan-Canadian Trust Framework Model (June 2019)
    d. Verified Organization Component Overview (November 2019)
    e. Verified Login Component Overview (November 2019)
    f. Verified Person Component Overview (November 2019)
4. Identity Management Sub-Committee (IMSC)
    a. Pan-Canadian Assurance Model (2010)
    b. Pan-Canadian Approach to Trusting Identities (2011)
5. Office of the Privacy Commissioner of Canada (OPC)
    a. Guidelines for Obtaining Meaningful Consent (May 2018)
6. Treasury Board of Canada Secretariat (TBS)
    a. Federating Identity Management in the Government of Canada (2011)
    b. Guideline on Defining Authentication Requirements (2012)
    c. Standard on Identity and Credential Assurance (2013)
    d. Guideline on Identity Assurance (2017)
    e. Directive on Identity Management (2019)
7. World Bank (WB)
    a. ID4D Practitioner's Guide (2019)
8. World Wide Web Consortium (W3C)
    a. Verifiable Credentials Data Model 1.0 (2019)

Individuals

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

1347