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

VERSION 1.3

CONSOLIDATED OVERVIEW

Document Version:	0.2
Document Status:	Consultation Draft
Date:	2021-04-21
Security Classification:	UNCLASSIFIED

DOCUMENT VERSION CONTROL

Version Number	Date of Issue	Author(s)	Brief Description
0.1	2021-01-14	ISED and TBS	Consultation Draft
0.2	2021-04-21	ISED and TBS	Consultation Draft

TABLE OF CONTENTS

DOCUMENT VERSION CONTROL III
TABLE OF CONTENTS V
LIST OF FIGURES IX
EXECUTIVE SUMMARY XI
1 INTRODUCTION 1
2 THE PAN-CANADIAN TRUST FRAMEWORK 3
2.1 OVERVIEW 3
2.1.1 Background *3*
2.1.2 What is the PCTF? *3*
2.1.3 Scope of the PCTF *4*
2.2 THE PCTF MODEL 5
2.3 NORMATIVE CORE 7
2.3.1 Digital Representations *7*
2.3.1.1 Entities 7
2.3.1.2 Relationships between Entities 8
2.3.1.3 Attributes 10
2.3.2 Identity Types *12*
2.3.3 Atomic and Compound Processes *12*
2.3.3.1 Atomic Processes 13
2.3.3.2 Compound Processes 15
2.3.4 Dependencies *16*
2.3.5 Conformance Criteria *16*
2.3.6 Qualifiers *16*
2.4 MUTUAL RECOGNITION 19
2.4.1 Process Mapping *19*
2.4.2 Alignment to Other Frameworks *20*
2.4.3 Assessment *21*
2.4.4 Acceptance *21*
2.5 SUPPORTING INFRASTRUCTURE 23
2.5.1 Methods *23*
2.5.2 Conveyance Mechanisms *24*
2.6 DIGITAL ECOSYSTEM ROLES AND INFORMATION FLOWS 25
2.6.1 Roles *25*
2.6.2 Information Flows *27*
2.7 ATOMIC PROCESSES IN DETAIL 29
2.7.1 Identity Domain Processes *29*
2.7.2 Relationship Domain Processes *33*
2.7.3 Credential Domain Processes *37*

2.7.4 Consent Domain Processes ... 41
2.7.5 Signature Domain Processes ... 45
2.8 Qualifiers in Detail ... 47
2.8.1 Identity Domain Qualifiers ... 47
2.8.2 Pan-Canadian Levels of Assurance (LOA) Qualifiers ... 47
2.8.3 Signature Domain Qualifiers ... 48
2.8.4 Other Trust Frameworks Qualifiers ... 49
3 APPENDIX A: TERMS AND DEFINITIONS ... 51
4 APPENDIX B: IDENTITY MANAGEMENT OVERVIEW ... 67
4.1 Identity ... 67
4.1.1 Real-World Identity ... 67
4.1.2 Identity in Identity Management ... 67
4.2 Defining the Population ... 68
4.3 Defining the Identity Context ... 68
4.4 Determining Identity Information Requirements ... 69
4.4.1 Identifier ... 70
4.4.2 Assigned Identifier ... 71
4.5 Identity Resolution ... 72
4.6 Ensuring the Accuracy of Identity Information ... 73
5 APPENDIX C: LEGAL ENTITIES ... 75
5.1 Types of Legal Entities ... 75
5.2 Treatment of Legal Entity Information ... 75
6 APPENDIX D: RELATIONSHIPS IN DETAIL ... 77
6.1 Relationship Models ... 77
6.1.1 Balanced Relationship ... 77
6.1.2 Agency Relationship ... 77
6.1.3 Directed Relationship ... 78
6.2 Relationships within an Organization ... 79
6.3 Organization to Organization Relationships ... 80
7 APPENDIX E: CREDENTIALS OVERVIEW ... 81
7.1 What is a Credential? ... 81
7.2 Types of Credentials ... 83
7.3 The PCTF Credential Model ... 84
7.4 Claims Assertion Models ... 86
7.4.1 The Claims Assertion Model of a Subject Claim ... 86
7.4.2 The Claims Assertion Model of a Relationship Claim ... 87
7.5 The Credential Issuance Model ... 88
8 APPENDIX F: IDENTITY VERIFICATION IN DETAIL ... 89
9 APPENDIX G: CREDENTIAL VERIFICATION IN DETAIL ... 91

9.1 AUTHENTICATORS 91

10 APPENDIX H: GUIDELINES ON MUTUAL RECOGNITION 93

10.1 PLANNING AND ENGAGEMENT 93

10.2 PROCESS MAPPING 94

10.3 ASSESSMENT 94

10.4 ACCEPTANCE 95

11 APPENDIX I: THEMATIC ISSUES 97

12 APPENDIX J: BIBLIOGRAPHY 99

LIST OF FIGURES

Figure 1: The Pan-Canadian Trust Framework Model 5
Figure 2: Atomic Entities and Compound Entities 8
Figure 3: A Network of Entities and Relationships 9
Figure 4: A Network of Compound Entities and Relationships 10
Figure 5: The Atomic Process Model 13
Figure 6: Examples of Atomic Processes (Modeled)..................... 14
Figure 7: Example of a Compound Process (Modeled)..................... 15
Figure 8: Supporting Infrastructure 23
Figure 9: Conveying Output States between Parties 24
Figure 10: Digital Ecosystem Roles and Information Flows 25
Figure 11: The Balanced Relationship Model 77
Figure 12: The Agency Relationship Model 77
Figure 13: The Directed Relationship Model 78
Figure 14: An Internal Relationship Network within an Organization..................... 79
Figure 15: Organization to Organization Relationships 80
Figure 16: The PCTF Credential Model 84
Figure 17: The Claims Assertion Model of a Subject Claim 86
Figure 18: The Claims Assertion Model of a Relationship Claim 87
Figure 19: The Credential Issuance Model 88

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 12** are a set of appendices which provide terms and definitions, more detailed information 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 the efficiency of 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 defines two types of *digital representations* that are essential for the development of the digital ecosystem:

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

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 allows for the use of different platforms, services, architectures, and technologies. The PCTF does not recommend one technology solution over another.

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, and certified to be trusted within the digital ecosystem.

1 INTRODUCTION

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

The audience for this document includes:

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

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

[1] 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.

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.[2] 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 methodology. It is not a “standard” as such, but is, instead, a framework that uses existing standards, policies, guidelines, and practices where available (e.g., security, privacy, service delivery) and specifies criteria for those areas where standards and policies do not exist.

The PCTF enables the alignment and assessment of business processes, thereby increasing confidence in identity solutions that are intended to work across organizational boundaries. 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 an identity solution and identifies any dependencies on external organizations.

The PCTF enables the recognition and acceptance of:

- Digital identities of entities; and
- Digital relationships between entities.

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

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

In addition, 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 PCTF is not a *governance* framework.

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.

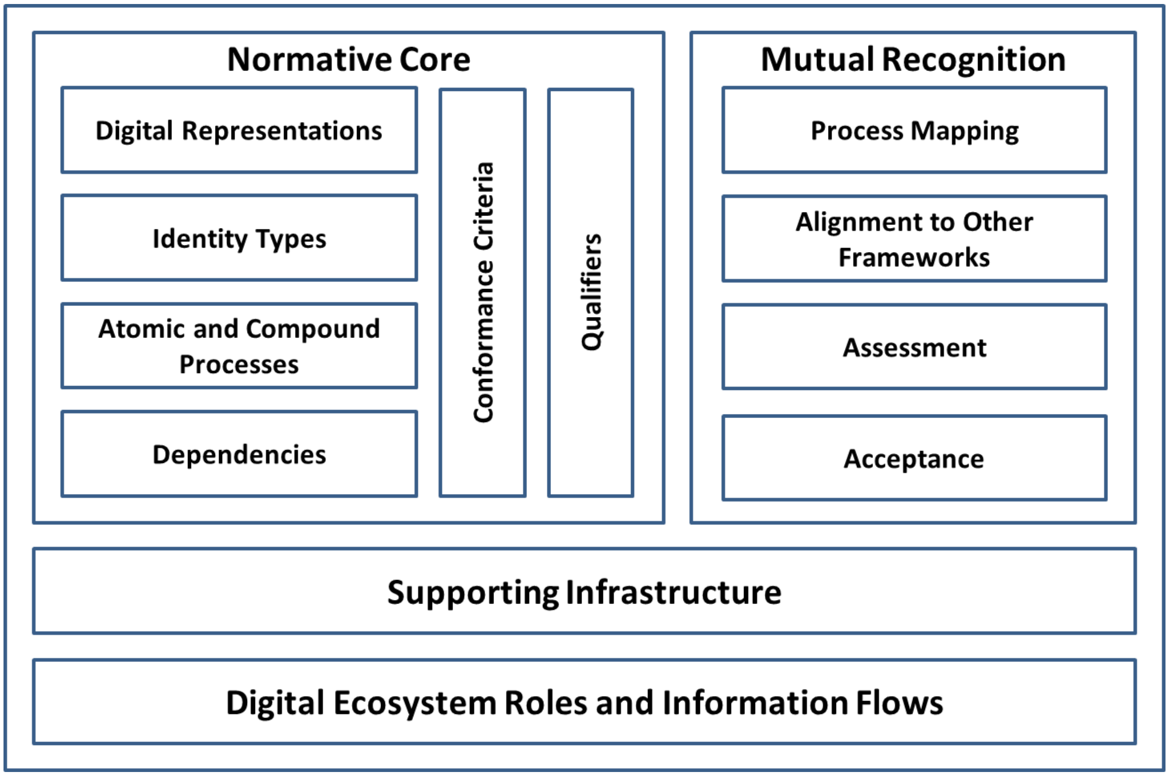


Figure 1: The Pan-Canadian Trust Framework Model

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 the 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 Digital Representations

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

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 an entity to other entities.

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. It is also anticipated that in the future the PCTF will be used to facilitate the mutual recognition of digital representations between countries.

2.3.1.1 Entities

An entity is a thing with a distinct and independent existence, such as a person or an organization, 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 of four roles (i.e., *Subject*, *Issuer*, *Holder*, or *Verifier*) in the digital ecosystem[3].

There are two types of entities: atomic entities and compound entities. An atomic entity is an entity that cannot be decomposed into smaller units. Persons are atomic entities. A compound entity is an entity that is comprised of one or more atomic entities. Organizations are compound entities. Figure 2 illustrates the two types of entities.

[3] See Section 2.6.1 for more information on the digital ecosystem roles.

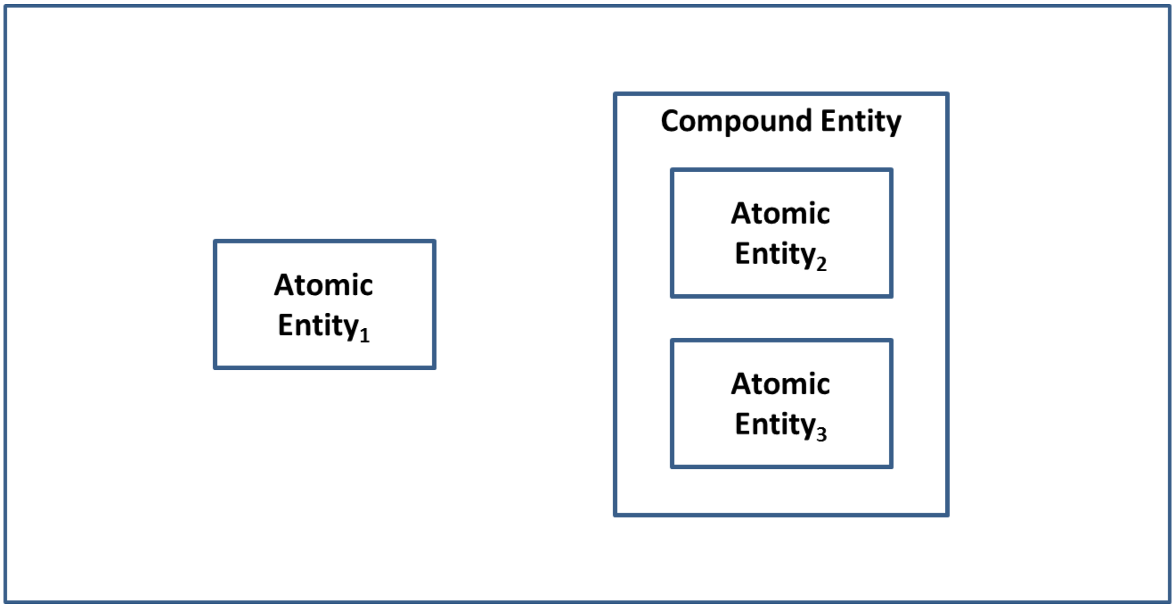


Figure 2: Atomic Entities and Compound Entities

2.3.1.2 Relationships between Entities

A relationship[4] is an association between two or more entities. The entities in the relationship can be any combination of atomic entities and compound entities[5]. Some examples of relationships are:

- Person to Person (e.g., a married couple)
- Person to Organization (e.g., an employee of a corporation)
- Organization to Organization (e.g., a subsidiary of a parent corporation)

Figure 3 illustrates a network of relationships between entities. Note that the entities in this diagram could be any combination of atomic entities and compound entities.

[4] For more detailed information on relationships see Appendix D.

[5] **Note**: Relationships between entities must be differentiated from interactions between entities (i.e., transaction execution). This concept will be discussed in more detail in a subsequent version of the PSP PCTF.

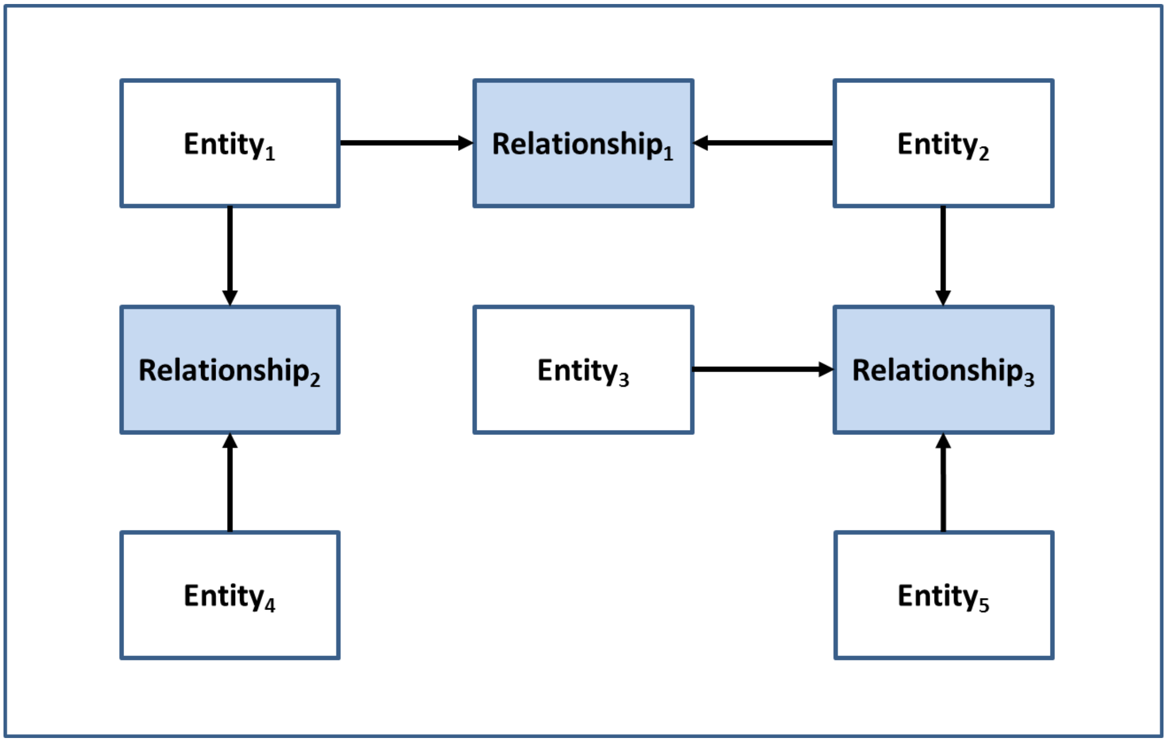


Figure 3: A Network of Entities and Relationships

Figure 4 shows a more detailed view of a network of relationships between two compound entities. Note that one of the compound entities has an internal network of relationships between two atomic entities.

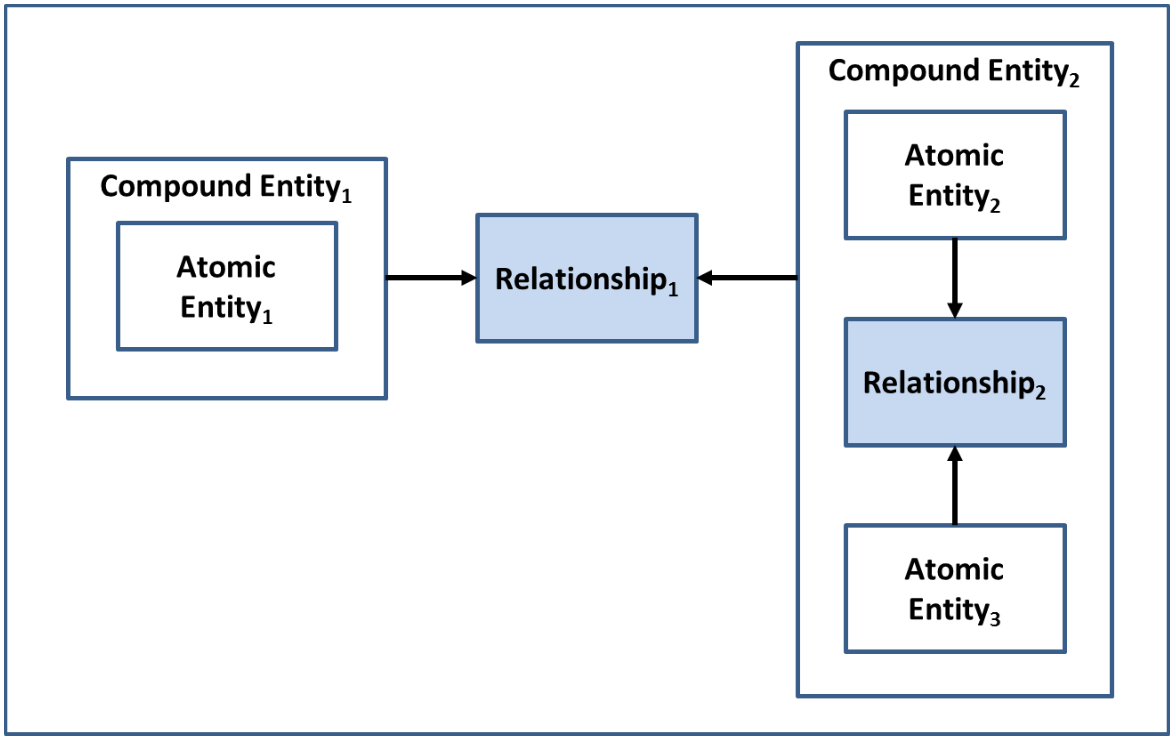


Figure 4: A Network of Compound Entities and Relationships

For more detailed information on relationships see Appendix D.

2.3.1.3 Attributes

An attribute is defined as a property or characteristic of a thing[6]. The PCTF recognizes three types of attributes: entity attributes, relationship attributes, and credential attributes. Entity attributes and relationship attributes are used to express Claims[7].

[6] There is a special kind of attribute that is referred to as a *derived predicate*. A derived predicate is an attribute that takes the form of a Boolean value (i.e., a "True" or "False" value) that is based upon the value(s) of one or more other attributes. For example, a derived predicate attribute such as "Aged21andOlder" contains a "True" or "False" value that indicates whether a person is twenty-one years of age or older, as opposed to containing the person's actual age or birth date. The use of a derived predicate better protects a person's privacy by disclosing only the minimum amount of personal information required to validate a person's eligibility for a service.

[7] For more information on Claims see Section 2.6.2 and Appendix E (Section 7.4).

An entity attribute is a property or characteristic of an entity. Some examples of entity attributes include:

- The full name of a person
- The legal name of a corporation
- The date of birth of a person
- The date of incorporation of a corporation
- The address of residence of a person
- The address of business of a corporation
- The driver's licence number of a person
- The logging permit number of a corporation

A relationship attribute is a property or characteristic of an association between two or more an entities. Some examples of relationship attributes include:

- The type of relationship (e.g., marriage, partnership, parent of a child, owner of a business)
- The sub-type of the relationship (e.g., sole proprietor of a business)
- The declaring authority
- The effective date
- The expiry date
- The status of the relationship (e.g., active, revoked)

A credential attribute[8] is a property or characteristic of a credential. Some examples of credential attributes include:

- The type of credential
- The Issuer of the credential
- The issuance date
- The expiry date
- The status of the credential (e.g., active, suspended, revoked)

[8] Credential attributes are also known as *Credential metadata*. See Appendix E for more information.

2.3.2 Identity Types

Within the identity domain, there are two types of identity: *foundational identity* and *contextual identity*.

- A **Foundational Identity** is an identity that has been established or changed as a result of a foundational event (e.g., birth, person legal name change, immigration, legal residency, naturalized citizenship, death, organization legal name registration, organization legal name change, or bankruptcy).
- A **Contextual Identity** is an identity that is used for a specific purpose within a specific identity context[9] (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 are under the exclusive control 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.

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

2.3.3 Atomic and Compound Processes

The PCTF defines a set of atomic processes that can be separately assessed and certified to be compatible with one another in a digital ecosystem. An atomic process is a set of logically related activities that results in a state transition[10]. 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.

[9] In delivering their programs and services, program/service providers operate within a certain environment or set of circumstances, which in 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.

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

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 four atomic processes – *Identity Information Determination*, *Identity Evidence Determination*, *Relationship Information Determination*, and *Relationship Evidence Determination* – are carried out only once for a program/service.

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 5 illustrates the atomic process model.

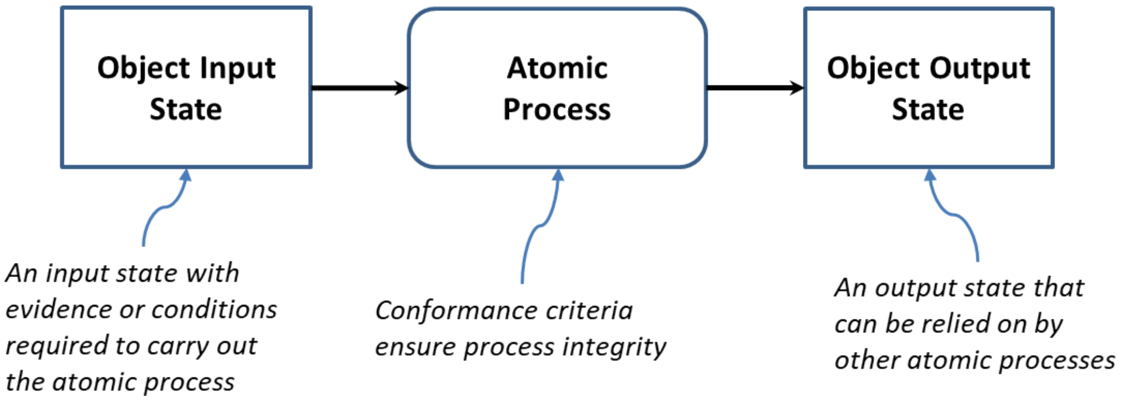

Object Input State
Atomic Process
Object Output State
An input state with evidence or conditions required to carry out the atomic process
Conformance criteria ensure process integrity
An output state that can be relied on by other atomic processes

Figure 5: The Atomic Process Model

Atomic processes are crucial building blocks to ensuring the overall integrity of the digital identity supply chain and therefore, the integrity of digital services. The integrity of an atomic process is paramount because the output of an atomic process is relied upon by many participants – across jurisdictional and public and private sector boundaries, and over the short term and the long term. The PCTF ensures the integrity of an atomic process through 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 an entity. The conformance criteria may specify that the party responsible for carrying out the atomic process must ensure that the identifier assigned to the entity is unique for a specified population.

The atomic processes are detailed in Section 2.7.

Figure 6 illustrates some model diagrams of three atomic processes.

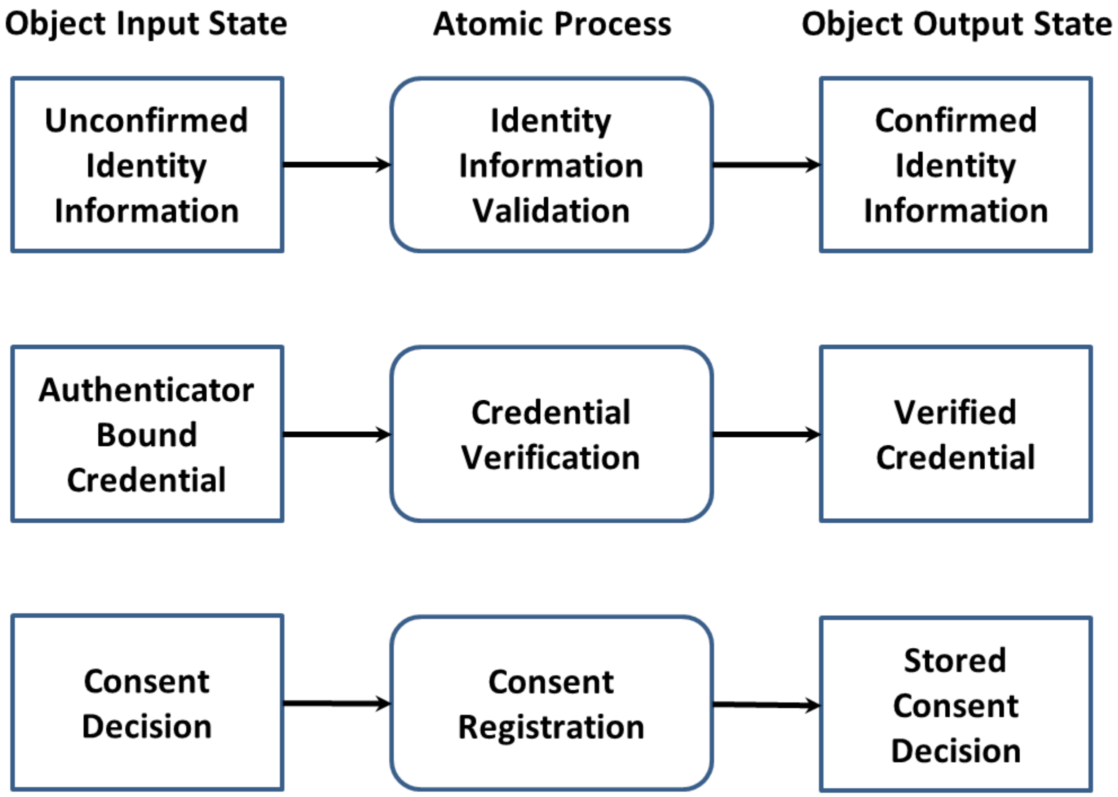


Figure 6: Examples of Atomic Processes (Modeled)

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 7.

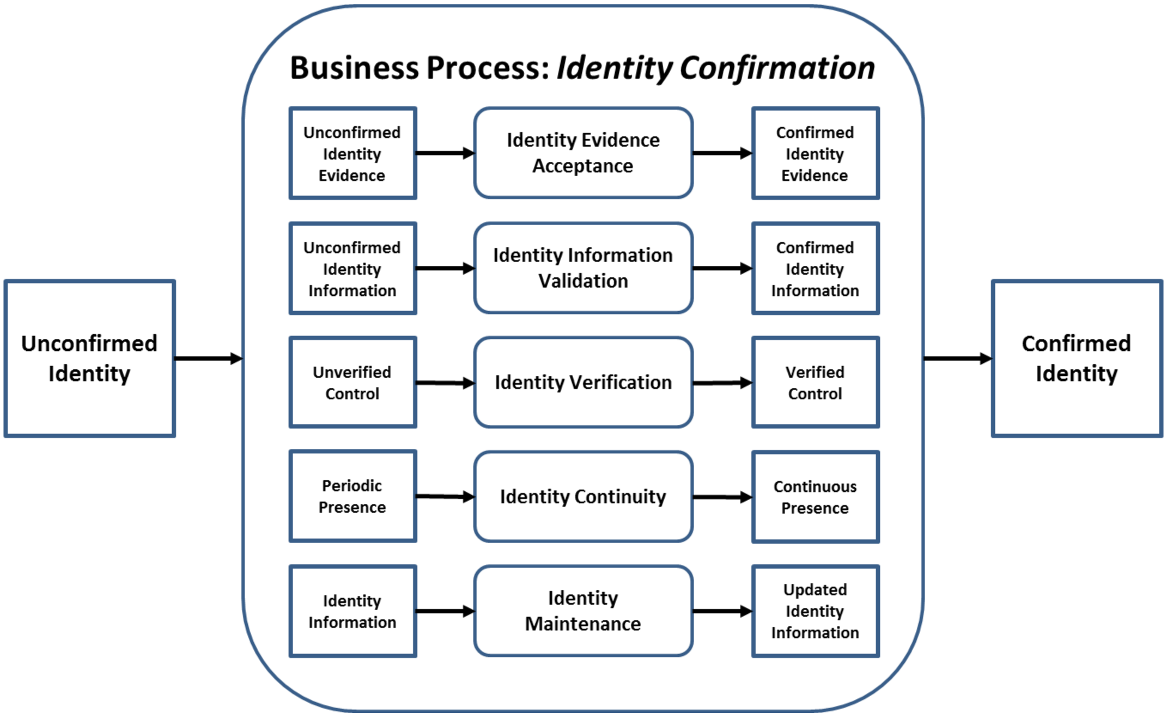

Business Process: *Identity Confirmation*
Unconfirmed Identity
Unconfirmed Identity Evidence
Identity Evidence Acceptance
Confirmed Identity Evidence
Unconfirmed Identity Information
Identity Information Validation
Confirmed Identity Information
Unverified Control
Identity Verification
Verified Control
Periodic Presence
Identity Continuity
Continuous Presence
Identity Information
Identity Maintenance
Updated Identity Information
Confirmed Identity

Figure 7: 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 an entity can be performed independently at any time, it is logically correct to do so only after *Identity Resolution* for that entity has been achieved. This type of dependency is specified in the conformance criteria (see Section 2.3.5).

The second type is dependencies on external organizations for the provision of atomic process outputs (e.g., a credential service provider). 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 an entity. The conformance criteria specify that the atomic process must ensure that the identifier that is assigned to the entity is unique for a specific population or context.

The conformance criteria are maintained in a separate document – the PSP PCTF Assessment Workbook. In the future, the conformance criteria may be embedded in an automated assessment tool.

2.3.6 Qualifiers

Qualifiers are assigned to conformance criteria. Qualifiers may indicate a level of confidence or stringency required, or they may indicate a specific requirement in relation to an identity domain requirement, a specific policy or regulatory requirement, or another trust framework. Qualifiers are used to select the applicable conformance criteria to be used in an assessment process.

Qualifiers can also be used to facilitate the mapping of conformance criteria equivalencies across different trust frameworks. In addition, qualifiers can be used 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 Secretariat of Canada.

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

See Section 2.8 for more detailed 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. 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.

The PSP PCTF Assessment Workbook (a separate document) has been developed to assist in the PCTF assessment process. This workbook consolidates the atomic processes and accompanying conformance criteria into a set of spreadsheets intended to aid in the mapping of existing business processes and to assist the assessment team in cross-referencing data for assessment analysis. Qualifiers are assigned to the conformance criteria to assist in the selection of the conformance criteria that are applicable to the assessment process[11].

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 the PCTF does not assume that a single Issuer or Verifier is solely responsible for all of the atomic processes. An organization may choose to outsource or delegate the responsibility of an atomic process to another party. 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.

[11] See Section 2.3.6 for more information on qualifiers.

Eventually, the PCTF acceptance process may include standard processes defined by the International Standards Organization (ISO)[12] as follows:

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

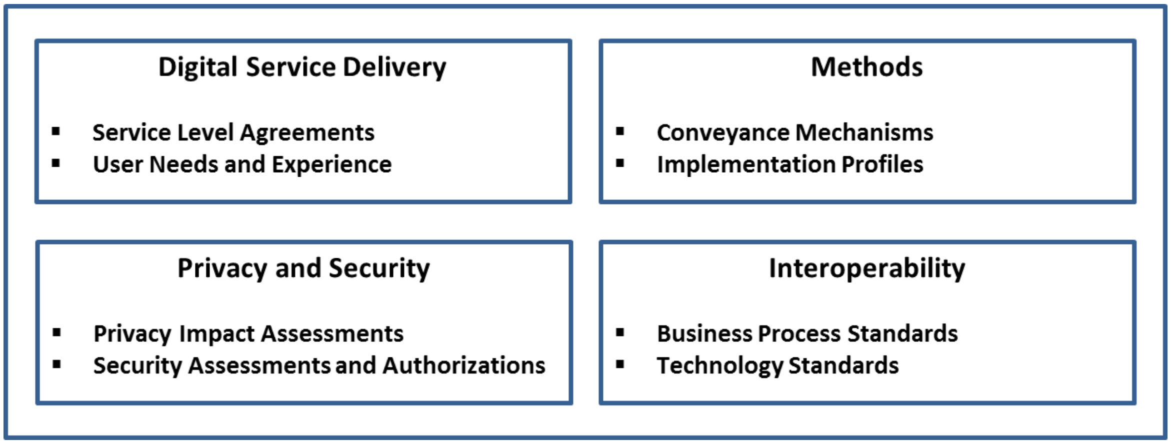
Formalized certification and accreditation programs are currently being developed. It is anticipated that once formalized, independent third parties will be enabled to conduct PCTF assessments. There are several domestic and international standards bodies that have recognized conformity assessment standards 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.

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

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 the 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 8 illustrates some elements (with examples) of what could constitute the Supporting Infrastructure.



Digital Service Delivery

- Service Level Agreements
- User Needs and Experience

Methods

- Conveyance Mechanisms
- Implementation Profiles

Privacy and Security

- Privacy Impact Assessments
- Security Assessments and Authorizations

Interoperability

- Business Process Standards
- Technology Standards

Figure 8: 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 are the sets of rules that govern how actors in the digital ecosystem interact directly or indirectly with one another. Methods encompass such things as data models and schemas, communications protocols, conveyance mechanisms[13], cryptographic algorithms, databases, distributed ledgers, verifiable data registries, and similar schemes; and combinations of these. Methods may also include systems that are isolated or have intermittent connectivity.

The PCTF does not recommend one Method over another.

[13] See Section 2.5.2.

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 9, the conveyance mechanisms are situated between the parties producing and consuming the output states of atomic processes.

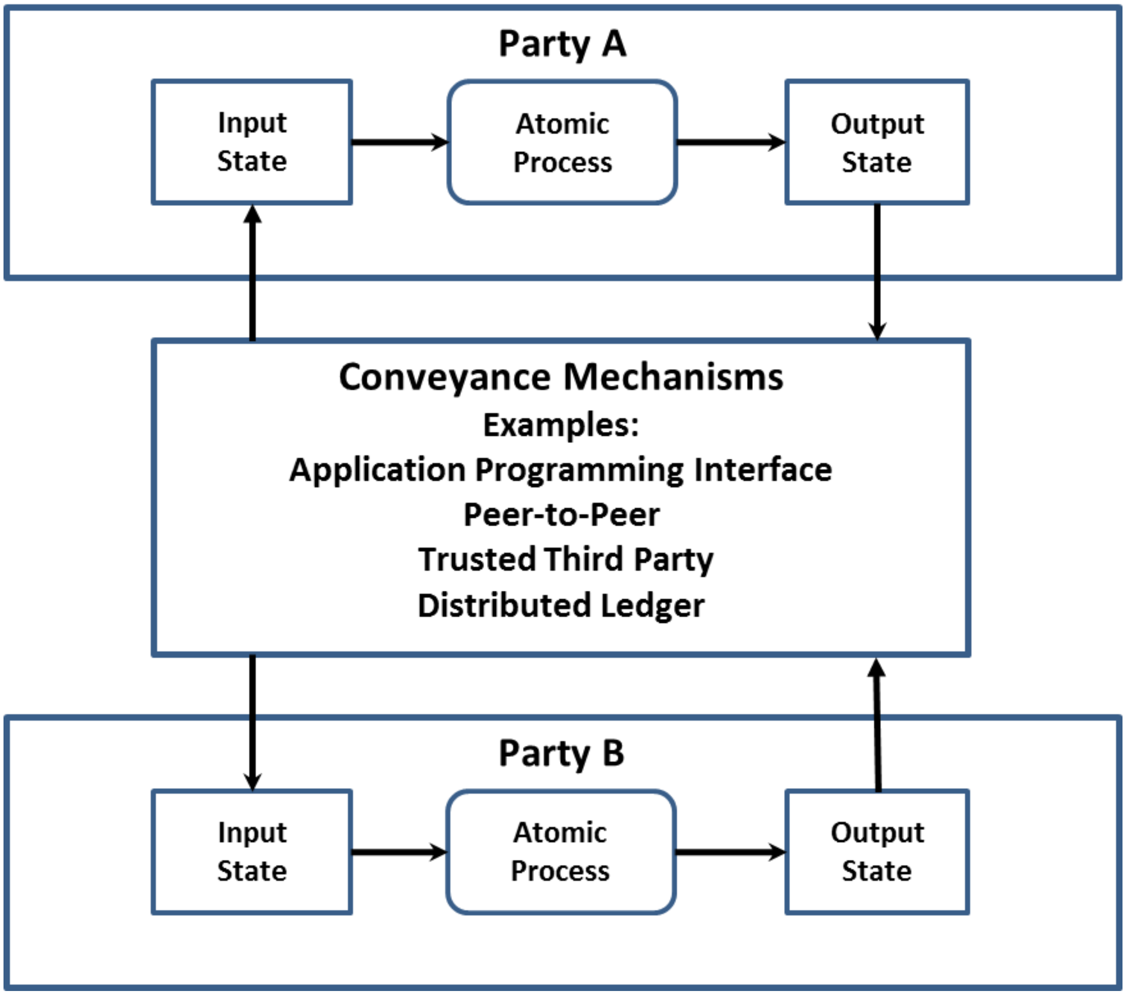


Figure 9: Conveying Output States between Parties

The PCTF does not recommend one conveyance mechanism over another. Moreover, the PCTF allows for the possibility of competing providers coexisting to serve the conveyance mechanism needs of different communities across the public and private sector.

2.6 Digital Ecosystem Roles and Information Flows

Figure 10 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.)

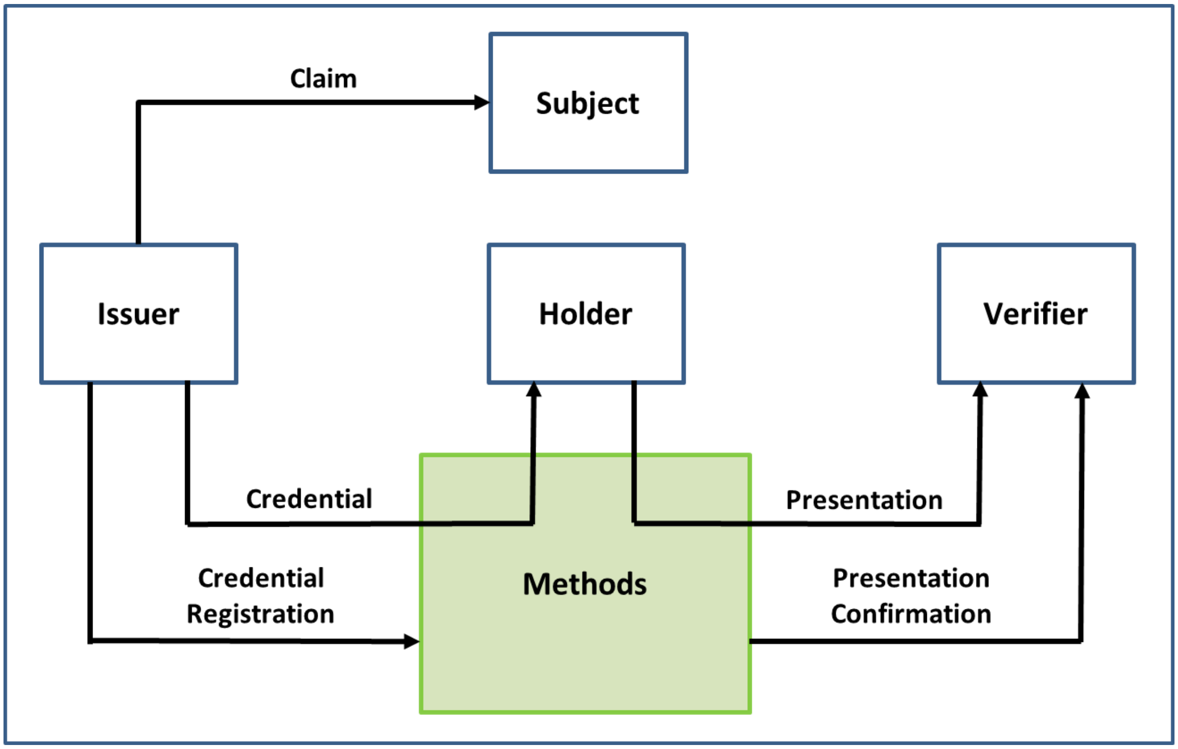


Figure 10: Digital Ecosystem Roles and Information Flows

2.6.1 Roles

The model consists of four roles:

1. **Subject:** An entity 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.

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[14].
4. **Verifier**: An entity that accepts a Presentation from a Holder for the purposes of delivering services or administering programs.

Traditionally, the digital ecosystem roles have been performed (in whole or in part) by many different entities acting under a variety of labels. These actors and their traditional roles can be assigned to the digital ecosystem roles as shown in the following table.

Role	Actors
Issuer	Authoritative Party, Identity Assurance Provider, Identity Service Provider, Credential Assurance Provider, Credential Service Provider, Credential Authenticator Provider, Digital Identity Service Provider, Delegated Service Provider, Producer
Subject	Person, Organization
Holder	Digital Identity Owner, Card Holder
Verifier	Relying Party, Credential Service Provider, Digital Identity Consumer, Delegated Service Provider, Consumer

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 service provider).

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

[14] 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

In addition, the model consists of five information flows:

1. **Claim:** A statement about a Subject or a statement about an association that exists between two or more Subjects. Claims are asserted by Issuers.
2. **Credential:** An assertion of identity, qualification, competence, authority, rights, privileges, permissions, status, eligibility, or asset ownership (or a combination of these). A credential contains a set of one or more Claims asserted about one or more Subjects[15].
3. **Presentation:** Information derived from one or more Credentials. The source Credentials may have been issued by different Issuers.
4. **Credential Registration:** A statement made by the Issuer that the Issuer issues a type of Credential. The statement may include a definition of the Credential's format.
5. **Presentation Confirmation:** A determination by the Verifier of the correctness[16] of the Presentation.

[15] An example of a Credential having more than one Subject is a marriage certificate.

[16] Correctness determination involves the acceptance by the Verifier of the authority of the Issuers of the Credentials that form the basis of the Presentation as well as ensuring that the source Credentials have not been tampered with.

2.7 Atomic Processes in Detail

2.7.1 Identity Domain Processes

Identity Information Determination

Process Description	Identity Information Determination is the process of determining the identity context[17], the identity information requirements[18], and the identifier[19].
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

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

[17] See Section 4.3 for more information.

[18] See Section 4.4 for more information.

[19] See Section 4.4.1 for more information.

Identity Evidence Acceptance

Process Description	Identity Evidence Acceptance 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

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

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[20].
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

[20] See Section 4.5 for more information.

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

Identity Verification

Process Description	Identity Verification is the process of confirming that the identity information is under the control of the Subject[21].
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

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

[21] For more information on Identity Verification see Appendix F.

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

Identity Linking

Process Description	Identity Linking is the process of mapping one or more assigned identifiers to a Subject.
Input State	**Unlinked Identity**: No assigned identifier has been mapped to the Subject
Output State	**Linked Identity**: One or more assigned identifiers have been mapped to the Subject

2.7.2 Relationship Domain Processes

Relationship Information Determination

Process Description	Relationship Information Determination is the process of determining the relationship context, the relationship information requirements, and the relationship identifier.
Input State	**No Determination Made**: The relationship context, the relationship information requirements, and the relationship identifier have not been determined
Output State	**Determination Made**: The relationship context, the relationship information requirements, and the relationship identifier have been determined

Relationship Evidence Determination

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

Relationship Evidence Acceptance

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

Relationship Information Validation

Process Description	Relationship Information Validation is the process of confirming the accuracy of information about a relationship between two or more Subjects as established by the Issuer.
Input State	**Unconfirmed Relationship Information**: The relationship information has not been confirmed with the Issuer
Output State	**Confirmed Relationship Information**: The relationship information has been confirmed with the Issuer

Relationship Resolution

Process Description	Relationship Resolution is the process of establishing the uniqueness of a relationship instance within a program/service population through the use of relationship information and identity information.
Input State	**Relationship and Identity Information**: The relationship information and the identity information may or may not be unique to one and only one relationship
Output State	**Unique Relationship and Identity Information**: The relationship information and the identity information is unique to one and only one relationship

Relationship Establishment

Process Description	Relationship Establishment is the process of creating a record of a relationship between two or more Subjects.
Input State	**No Record of Relationship**: No record of a relationship exists
Output State	**Record of Relationship**: A record of a relationship exists

Relationship Verification

Process Description	Relationship Verification is the process of confirming that the relationship information is under the control of the Subjects.
Input State	**Unverified Control**: The relationship information has not been verified as being under the control of the Subjects
Output State	**Verified Control**: The relationship information has been verified as being under the control of the Subjects

Relationship Continuity

Process Description	Relationship Continuity is the process of dynamically confirming that a relationship between two or more Subjects has a continuous existence over time.
Input State	**Periodic Presence**: The relationship exists sporadically and often only in association with a vital event or a business event (e.g., birth, marriage, acquisition)
Output State	**Continuous Presence**: The relationship exists continuously over time in association with many transactions

Relationship Maintenance

Process Description	Relationship Maintenance is the process of ensuring that the information about a relationship between two or more Subjects is accurate, complete, and up-to-date.
Input State	**Relationship Information**: The relationship information is not up-to-date
Output State	**Updated Relationship Information**: The relationship information is up-to-date

Relationship Suspension

Process Description	Relationship Suspension is the process of flagging a record of a relationship as temporarily no longer in effect.
Input State	**Record of Relationship**: A record of a relationship exists
Output State	**Suspended Relationship**: The relationship is temporarily no longer in effect

Relationship Reinstatement

Process Description	Relationship Reinstatement is the process of transforming a suspended relationship back to an active state.
Input State	**Suspended Relationship**: The record of a relationship is temporarily no longer in effect
Output State	**Updated Record of Relationship**: The record of a relationship has been updated

Relationship Revocation

Process Description	Relationship Revocation is the process of flagging a record of a relationship as no longer in effect.
Input State	**Record of Relationship**: A record of a relationship exists
Output State	**Revoked Relationship**: The relationship is no longer in effect

2.7.3 Credential Domain Processes

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	**No Credential**: No claims have been associated with the credential
Output State	**Issued Credential**: One or more Claims about one or more Subjects have been associated with the Credential and the Credential has been assigned to a Holder

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 credential verifications, 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

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	**Issued Credential**: A Credential has been assigned to a Holder
Output State	**Validated Credential**: The issued Credential is valid

Credential Verification

Process Description	Credential Verification is the process of verifying that a Holder has control over an issued Credential[22]. 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

Credential Maintenance

Process Description	Credential Maintenance is the process of updating the credential attributes (e.g., expiry date, status of the credential) 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

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

[22] For more information on Credential Verification see Appendix G.

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

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

2.7.4 Consent Domain Processes

Consent Notice Formulation

Process Description	Consent Notice Formulation is the process of producing a consent 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 consent notice statement is applicable; and under whose jurisdiction or authority the consent notice statement is issued. This process should be carried out in accordance with any requirements of jurisdictional legislation and regulation.
Input State	**No Consent Notice Statement**: No consent notice statement exists
Output State	**Consent Notice Statement**: A consent notice statement exists

Consent Notice Presentation

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

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 consent notice statement, resulting in either a “yes” or “no” consent decision.
Input State	**Presented Consent Notice Statement**: A consent notice statement has been presented to a person
Output State	**Consent Decision**: A consent decision exists

Consent Registration

Process Description	Consent Registration is the process of storing the consent notice statement and the person's related consent decision. In addition, information about the person, the version of the consent notice statement that was presented, the date and time that the consent 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

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

Consent Renewal

Process Description	Consent Renewal is the process of extending the validity period 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

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

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

2.7.5 Signature Domain Processes

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

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

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**: 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). The establishment and maintenance of foundational identities are under the exclusive control 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**: 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 established and maintained by both the public and private sectors.

2.8.2 Pan-Canadian Levels of Assurance (LOA) Qualifiers

Pan-Canadian Identity Assurance Levels (Persons)	
Qualifier	**Description**
IP1	Little confidence required that a person is who they claim to be.
IP2	Some confidence required that a person is who they claim to be.
IP3	High confidence required that a person is who they claim to be.
IP4	Very high confidence required that a person is who they claim to be.

Pan-Canadian Identity Assurance Levels (Organizations)	
Qualifier	**Description**
IO1	Little confidence required that the organization identity information is correct.
IO2	Some confidence required that the organization identity information is correct.
IO3	High confidence required that the organization identity information is correct.
IO4	Very high confidence required that the organization identity information is correct.

Pan-Canadian Relationship Assurance Levels	
Qualifier	**Description**
R1	Little confidence required that the person(s) is/are who they claim to be, that the organization(s) identity information is correct, and that there is evidence of the relationship.
R2	Some confidence required that the person(s) is/are who they claim to be, that the organization(s) identity information is correct, and that there is evidence of the relationship.
R3	High confidence required that the person(s) is/are who they claim to be, that the organization(s) identity information is correct, and that there is evidence of the relationship.
R4	Very high confidence required that the person(s) is/are who they claim to be, that the organization(s) identity information is correct, and that there is evidence of the relationship.

Pan-Canadian Credential Assurance Levels	
Qualifier	**Description**
C1	Little confidence required that a Holder has control over an issued Credential and that the issued Credential is valid.
C2	Some confidence required that a Holder has control over an issued Credential and that the issued Credential is valid.
C3	High confidence required that a Holder has control over an issued Credential and that the issued Credential is valid.
C4	Very high confidence required that a Holder has control over an issued Credential and that the issued Credential is valid.

2.8.3 Signature Domain 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 signature domain 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**: Low 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 domain processes.
- **Authenticator Assurance Level (AAL)**: Refers to the credential verification process.
- **Federation Assurance Level (FAL)**: Refers to the strength of an assertion in a federated environment, used to communicate authenticator assurance and identity 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
agency relationship	A special case of a balanced relationship where the entities are equals, but where one entity (the principal) appoints another entity (the agent) to act on the principal's behalf for a specified purpose (e.g., power of attorney, an accounting firm filing taxes for a corporation). See also "balanced relationship".
agent	A person acting on behalf of an entity.
assigned identifier	A numeric or alphanumeric string that is generated automatically and that uniquely distinguishes between entities within a population 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 entity	An entity that cannot be decomposed into smaller units. Persons are atomic entities. See also "compound entity".
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 of a thing. See also "entity attribute", "relationship attribute", "credential attribute", and "identity attribute".
authentication	See "credential verification".

Term	Definition
authenticator	Something that a Holder controls that is used to prove that the Holder has retained control over an issued Credential.
authoritative source	A set of records maintained by an authority that meets established criteria.
balanced relationship	A relationship where the entities are equals (e.g., spouses in a marriage, partners in a business, corporations in a joint venture). See also “agency relationship”.
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 or a statement about an association that exists between two or more Subjects. A Claim is expressed by means of one or more attributes.

Term	Definition
	Claims are asserted by Issuers. See also "Subject Claim" and "Relationship Claim".
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 entity	An entity that is comprised of one or more atomic entities. Organizations are compound entities. See also "atomic entity".
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.
consent notice formulation	The process of producing a consent 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 consent notice statement is applicable; and under whose jurisdiction or authority the consent notice statement is issued. This process should be carried out in accordance with any requirements of jurisdictional legislation and regulation.
consent notice presentation	The process of presenting a consent notice statement to a person.
consent registration	The process of storing the consent notice statement and the person's related consent decision. In addition, information about the person, the version of the

Term	Definition
	consent notice statement that was presented, the date and time that the consent 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 period 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 consent 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).
Credential	An assertion of identity, qualification, competence, authority, rights, privileges, permissions, status, eligibility, or asset ownership (or a combination of these). A credential contains a set of one or more Claims asserted about one or more Subjects.
credential assurance	Confidence that a Holder has 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 control over an issued Credential and that the issued Credential is valid.
credential attribute	A property or characteristic of a credential.
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 credential verifications, 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 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, status of the credential) of an issued Credential.
Credential Metadata	One or more credential attributes that describe the properties or characteristics of the credential.
Credential Payload	A set of one or more Claims asserted about one or more Subjects.
Credential Proofs	One or more methods or mechanisms that are used to verify that the Issuer authored the Credential and that the Credential has not been tampered with.
credential recovery	The process of transforming a suspended Credential back to a usable state (i.e., an issued Credential).
Credential Registration	A statement made by the Issuer that the Issuer issues a type of Credential. The statement may include a definition of the Credential’s format.
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.

Term	Definition
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.
credential verification	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 can be used to generate a level of assurance.
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 an entity to other entities.
digital representation	An electronic representation of an entity or an electronic representation of the relationship between two or more entities.
directed relationship	A relationship where the entities are not equals (e.g., parent and child, parent corporation and subsidiary corporation, manager and subordinate).
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.

Term	Definition
entity	A thing with a distinct and independent existence, such as a person or an organization, 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 of four roles (i.e., Subject, Issuer, Holder, or Verifier) in the digital ecosystem.
entity attribute	A property or characteristic of an entity.
evidence of contextual identity	Evidence of identity that corroborates the evidence of foundational identity and assists in linking the identity information to a person. It may also provide additional information such as a photo, signature, or address. Examples include social insurance records; records of entitlement to travel, drive, or obtain health services; 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.

Term	Definition
	See “evidence of foundational identity” and “evidence of contextual identity”.
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 organizations and persons, respectively. By law both

Term	Definition
	business events and vital events must be recorded with a government entity and are subject to legislation and 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 entity within a population.
identity	A reference or designation used to uniquely distinguish a particular entity. There are two types of identity: foundational and contextual. See "foundational identity" and "contextual identity".
identity assurance (of an organization)	Confidence that the organization identity information is correct.
identity assurance (of a person)	Confidence that a person is who they claim to be.
identity assurance level (of an organization)	The level of confidence that the organization identity information is correct.
identity assurance level (of a person)	The level of confidence that a person is who they claim to be.
identity attribute	A property or characteristic associated with an identifiable entity (also known as "identity data element"). The Identity attributes of an entity are a subset of the entity's entity attributes.
identity context	The environment or set of circumstances within which

Term	Definition
	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 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 acceptance	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 an entity 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).

Term	Definition
identity information retrieval	The disclosure of identity information about an entity 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.
identity linking	The process of mapping one or more assigned identifiers to a 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.
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 entity presenting the identity information is in control of the identity. Knowledge-based confirmation is achieved by means of the challenge-response model: the entity 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

Term	Definition
	key, mailed-out access code, password, personal identification number, assigned identifier).
legal name	See “foundation name”, “primary name”.
legal presence	Lawful entitlement to be or reside in Canada.
Methods	The sets of rules that govern how actors in the digital ecosystem interact directly or indirectly with one another. Methods encompass such things as data models and schemas, communications protocols, conveyance mechanisms, cryptographic algorithms, databases, distributed ledgers, verifiable data registries, 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.
organization	A legal entity that is not a human being (referred to in law as a “juridical person”).
organizational information	Information about an identifiable organization.
person	A human being (referred to in law as 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.
physical possession confirmation	An identity verification method that requires physical possession or presentation of evidence to prove that the entity 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 source Credentials may have been issued by different Issuers.
Presentation Confirmation	A determination by the Verifier of the correctness of the

Term	Definition
	Presentation.
primary name	The name that a person or organization uses for formal and legal purposes (also known as "legal name"). See also "foundation name".
relationship	An association between two or more entities.
relationship assurance	Confidence that the person(s) is/are who they claim to be, that the organization(s) identity information is correct, and that there is evidence of the relationship.
relationship assurance level	The level of confidence that the person(s) is/are who they claim to be, that the organization(s) identity information is correct, and that there is evidence of the relationship.
relationship attribute	A property or characteristic of an association between two or more an entities.
Relationship Claim	A statement about an association that exists between two or more Subjects. A Relationship Claim is expressed by means of one or more relationship attributes.
relationship continuity	The process of dynamically confirming that a relationship between two or more Subjects has a continuous existence over time.
relationship establishment	The process of creating a record of a relationship between two or more Subjects.
relationship evidence determination	The process of determining the acceptable evidence of a relationship (whether physical or electronic).
relationship evidence acceptance	The process of confirming that the evidence of a relationship presented (whether physical or electronic) is acceptable.
relationship identifier	The set of identifiers of the parties in the relationship and the *relationship type* relationship attribute.
relationship information	The set of relationship attributes that describes the association between two or more entities.
relationship information determination	The process of determining the relationship context, the relationship information requirements, and the

Term	Definition
	relationship identifier.
relationship information validation	The process of confirming the accuracy of information about a relationship between two or more Subjects as established by the Issuer.
relationship maintenance	The process of ensuring that the information about a relationship between two or more Subjects is accurate, complete, and up-to-date.
relationship reinstatement	The process of transforming a suspended relationship back to an active state.
relationship resolution	The process of establishing the uniqueness of a relationship instance within a program/service population through the use of relationship information and identity information.
relationship revocation	The process of flagging a record of a relationship as no longer being in effect.
relationship suspension	The process of flagging a record of a relationship as temporarily no longer in effect.
relationship verification	The process of confirming that the relationship information is under the control of the Subjects.
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.
Subject Claim	A statement about a Subject. A Subject Claim is expressed by means of one or more entity attributes.

Term	Definition
trust framework	A set of agreed on principles, definitions, standards, specifications, conformance criteria, and assessment approach.
trusted referee confirmation	An identity verification method that relies on a trusted referee to prove that the entity 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.
user	See “Holder”.
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.

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 keep track of people and things… 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."

Joe Andrieu, *A Primer on Functional Identity*[23]

4.1.2 Identity in Identity Management

The concept of identity in identity management has a much stricter definition than real-world notions of identity. In identity management, identity is defined as a reference or designation used to uniquely distinguish a particular entity.

An identity must be unique[24]. This means that each entity can be distinguished from all other entities within a population of interest and that, when required, each entity can be uniquely identified. The uniqueness requirement ensures that a program or service can be delivered to a specific entity and that a program or service is delivered to the right entity.

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

[24] 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

Those entities that fall within the mandate of a program or service constitute the population of the program or service[25].

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 identity management is referred to as the identity context. Identity context is determined by factors such as mandate, target population (i.e., clients, customer base), and other responsibilities prescribed by legislation or agreements.

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

[25] The characteristics of a program/service population are a key factor in determining identity context. See section 4.3.

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 entity 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 entities within the program/service population (i.e., achieve the uniqueness requirement for identity); and
- Sufficient to describe the entity 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[26]. 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 entity 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*[27] (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 entity 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.

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

[27] See section 4.4.2.

- **Uniqueness** – The values associated with the identity attributes must be sufficiently different for each entity within the program/service population that the entities 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 within 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[28] 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 an entity at the time of identity establishment.

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

However, before an assigned identifier can be associated with an entity, the uniqueness of the entity'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 entity within a population.

Once associated with an entity, an assigned identifier uniquely distinguishes that entity from all other entities within 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 entities 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 an entity 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 entity 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[29]. Accuracy ensures the quality of identity information. It ensures that the information represents what is true about an entity, 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 key events (e.g., death of a person, dissolution of a corporation), may change over time. Ongoing updates to identity information may be required; otherwise, it becomes incorrect.
- **The identity information relates to a real entity**. Identity information must be associated with an entity which actually exists or existed at some point in time.
- **The identity information relates to the correct entity.** In large populations, entities may have the same or similar identity information as other entities within the population. While the requirement for identity uniqueness addresses this issue, the possibility of relating identity information to the wrong entity 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 comparing it to 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.

[29] 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].

5 APPENDIX C: LEGAL ENTITIES

5.1 Types of Legal Entities

Canadian law recognizes two kinds of legal entities: human beings which are referred to as *natural persons*, and non-human entities such as corporations, partnerships, funds, trusts, cooperatives, registered charities, governments, etc., that are treated in law as if they were natural persons. The Pan-Canadian Trust Framework refers to these two types of legal entities as persons and organizations respectively.

5.2 Treatment of 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 – although some organizational information may be protected by confidentiality agreements.

6 APPENDIX D: RELATIONSHIPS IN DETAIL

6.1 Relationship Models

6.1.1 Balanced Relationship

A balanced relationship is a relationship where the entities are equals (i.e., the power distribution among the entities is symmetric) (e.g., spouses in a marriage, partners in a business, corporations in a joint venture).

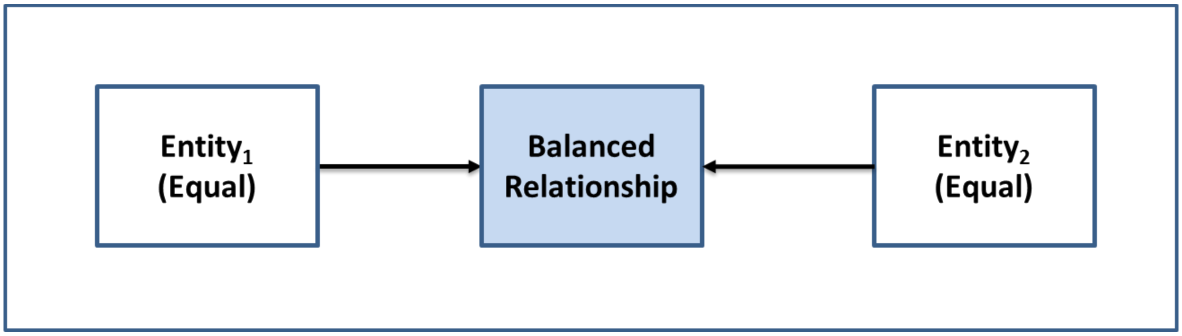


Figure 11: The Balanced Relationship Model

6.1.2 Agency Relationship

An agency relationship is a special case of a balanced relationship where the entities are equals, but where one entity (the principal) appoints another entity (the agent) to act on the principal's behalf for a specified purpose (e.g., power of attorney, an accounting firm filing taxes for a corporation).

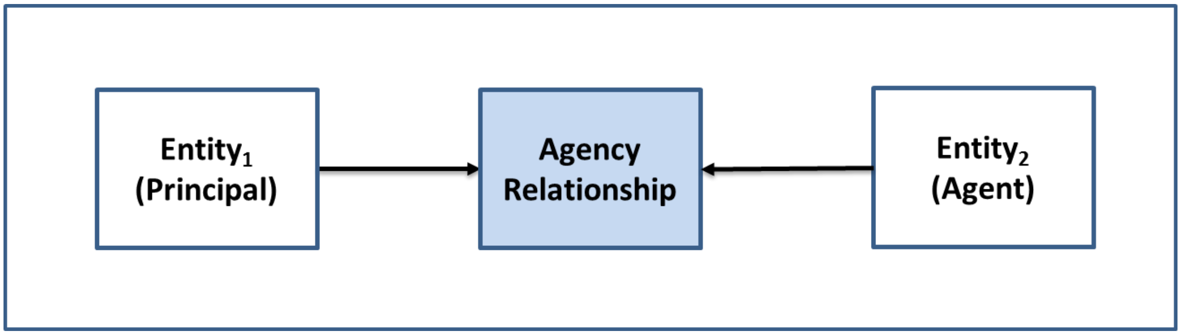


Figure 12: The Agency Relationship Model

The relationship between a principal and an agent is a contractual one. Therefore, rights and duties of the agent and principal are in accordance with the agency contract. To establish an agency, there must be consent of both the principal and the agent, although such consent may be implied rather than expressed.

The authorization by which the principal appoints another as an agent and confers upon the agent the authority to perform certain acts on behalf of the principal can be any type of contract or agreement. Hiring a real estate agent, an attorney, an administrative assistant are all forms of agency establishment.

6.1.3 Directed Relationship

A directed relationship is a relationship where the entities are not equals (i.e., the power distribution among the entities is asymmetric) (e.g., parent and child, parent corporation and subsidiary corporation, manager and subordinate).

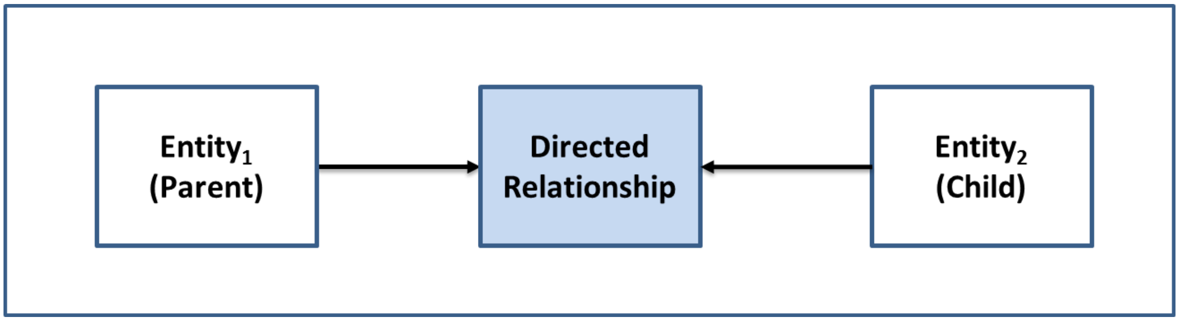


Figure 13: The Directed Relationship Model

6.2 Relationships within an Organization

The relationships between the atomic entities (persons) that exist within a compound entity (an organization) can form a complex network. Each relationship in the network can be identified as either a balanced or a directed relationship[30]. This is illustrated in Figure 14.

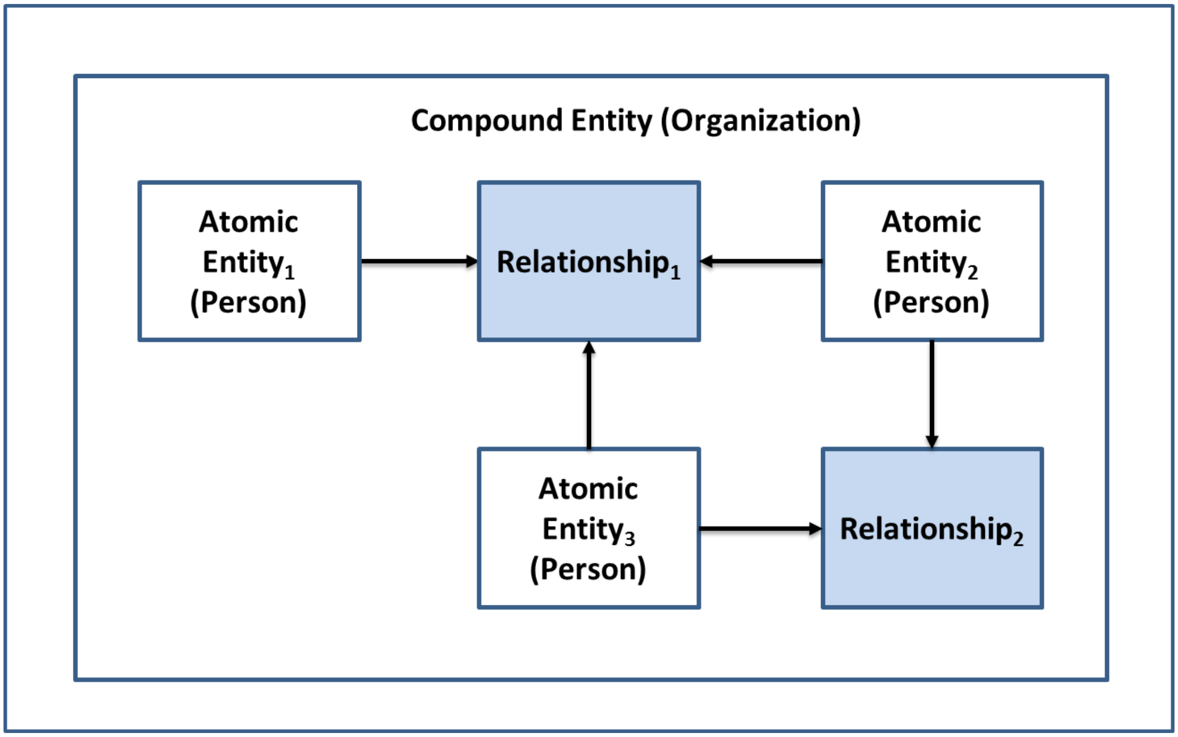

Compound Entity (Organization)
Atomic Entity$_1$ (Person)
Relationship$_1$
Atomic Entity$_2$ (Person)
Atomic Entity$_3$ (Person)
Relationship$_2$

Figure 14: An Internal Relationship Network within an Organization

[30] Agency relationships can exist within an organization, but they are probably rare. It might be argued that a manager could be viewed as the principal and their subordinate as the agent. However, when analyzed closely this example of an agency relationship probably acquires the entity inequality aspect of a directed relationship and should be considered as such.

6.3 Organization to Organization Relationships

Compound entities such as organizations can have relationships with other organizations and the network that these relationships form can be fairly complex. Moreover, these networks often contain all three relationship models and as a result an organization might take on more than one relationship role. This is illustrated in Figure 15.

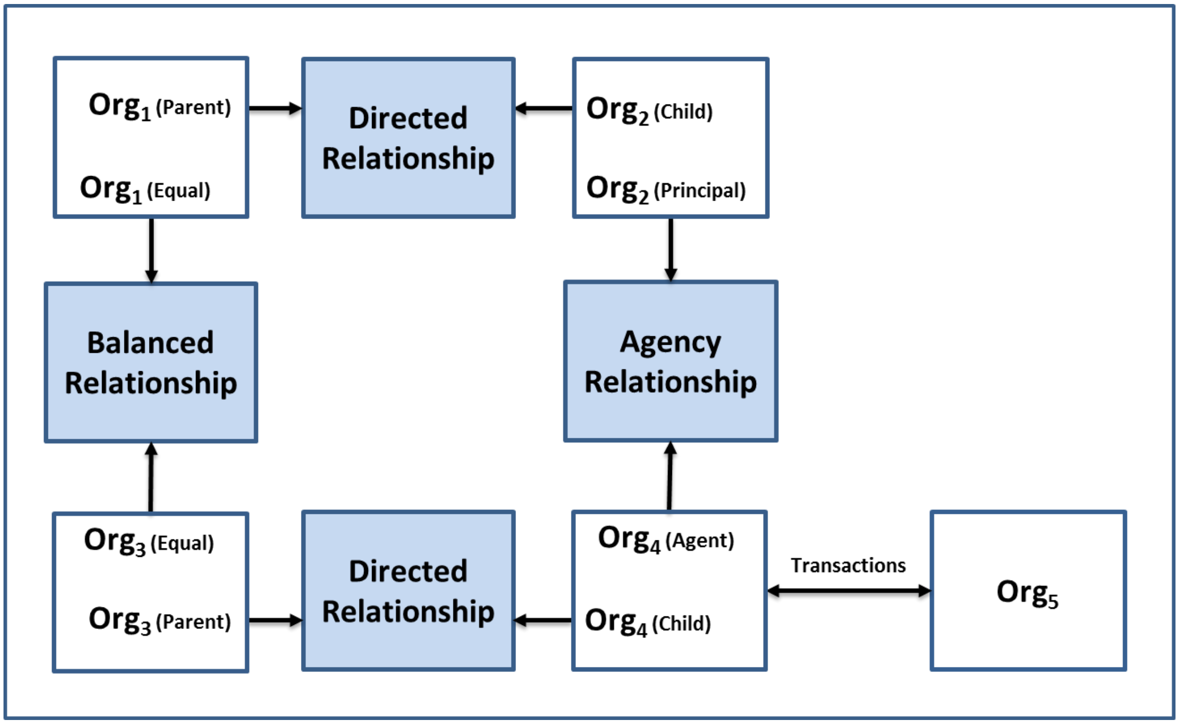


Figure 15: Organization to Organization Relationships

It should be noted that relationships between entities must be differentiated from interactions between entities (i.e., transaction execution). In Figure 15 above, **Org$_4$** has interactions with **Org$_5$**, but **Org$_4$** does not have a relationship with **Org$_5$**. This concept will be discussed in more detail in a subsequent version of the PSP PCTF.

7 APPENDIX E: CREDENTIALS OVERVIEW

7.1 What is a Credential?

The foundation of any transaction is trust. Trust is built on the assurance that any claim made by a transacting entity can be relied on as being true. As examples, a transacting entity may need to confirm the identity of the other entity with which it is transacting, whether that other entity has the authority to conduct a certain activity, or whether that other entity owns a particular asset.

Over time many types of credentials[31] have been developed and issued in order to solve the trust problem between entities. These credentials help to answer questions such as: "is this person permitted to drive a car in Ontario?", "does this person meet the requirements needed to receive employment insurance benefits?", "is this business licensed to cut timber in British Columbia?", or "does this business qualify for a small business loan?"

In the most general sense, a credential is an assertion of identity, qualification, competence, authority, rights, privileges, permissions, status, eligibility, or asset ownership (or a combination of these). More specifically, a credential contains a set of one or more *Claims* asserted about one or more *Subjects*[32]. The credential is issued by one entity, the *Issuer*, to another entity, the *Holder*. The Issuer either possesses the de jure authority to issue the credential, or is granted through convention and consensus the de facto authority and assumed competence to issue the credential.

Credentials contain two basic types of information. The first type of information is information about the credential itself[33]:

- Information that specifies the type of credential;
- Information that identifies the Issuer of the credential;
- Information that specifies the date that the credential was issued;
- Information that specifies any constraints on the credential (e.g., an expiry date, terms of use); and
- Information about the status of the credential (i.e., whether the credential is active, suspended, or revoked).

[31] See Section 7.2.

[32] For more information on the digital ecosystem roles and information flows, see section 2.6.

[33] This type of information is expressed by means of credential attributes. See section 2.3.1.3.

The second type of information contained within a credential consists of a set of attributes that describe the properties or characteristics of the entities who are the Subjects of the credential. These entity attributes are a combination of identity attributes[34] of the Subjects and non-identity attributes of the Subjects[35]. Some examples of non-identity attributes of a Subject are: the Subject's language of preference, the Subject's address of residence, and the Subject's total assets. In addition, the non-identity attributes of a Subject contained within a credential often provide credential-specific non-identity information about the Subject, either directly or indirectly (e.g., the nationality of the Subject, the Subject has obtained a Master's degree in electrical engineering from ABC University, the classes of motor vehicle that the Subject is authorized to operate). If a credential asserts that there is a *relationship* between the Subjects, then the credential will also include relationship attributes[36]. All of these various attributes are used to express one or more Claims about a Subject.

[34] A *pseudonymous credential* (a.k.a. an *anonymous credential*) is a credential that, while still making an assertion about an entity, does not reveal the entity's identity. A credential may contain identity attributes (such as an assigned identifier) but still be treated as a pseudonymous credential if the identity attributes are not intended to be used for identity resolution purposes. Pseudonymous credentials provide entities with a means to prove statements about themselves and their relationships with other entities while maintaining their anonymity.

[35] For more information on the distinction between identity attributes and non-entity attributes, see Appendix B (Section 4.4).

[36] For a general discussion of entities, relationships, and attributes, see Section 2.3.1.

7.2 Types of Credentials

The following is list of the many types of credentials that exist, along with some examples of their *documentation*[37]:

- Citizenship and Legal Residency Credentials (e.g., birth certificate, citizenship certificate, permanent residence certificate, passport)
- Service Enrolment Credentials (e.g., Provincial/Territorial health services card, private health services insurance card, private dental services insurance card, private travel insurance card, loyalty reward program card, group or club membership card)
- Operator Licensing Credentials (e.g., automobile driver's licence, heavy equipment operator’s licence)
- Business Credentials (e.g., licences, permits, inspection certificates)
- Financial Services Credentials (e.g., bank debit card, credit card)
- Asset Ownership Credentials (e.g., motor vehicle registration, deed to a property, proof of motor vehicle insurance)
- Academic Credentials (e.g., diploma, degree, certificate, certification, school transcript)
- Employment Credentials (e.g., letter of employment)
- Trade or Professional Membership Credentials (e.g., Union of Electricians membership card)
- Diplomatic Credentials (e.g., ambassadorial letters of introduction)
- Journalist Credentials (e.g., press pass)
- Security Clearance Credentials (e.g., building access pass, secure zone access pass)
- Authentication Credentials[38] (e.g., user name/password combination)

[37] See Section 7.3.

[38] Information systems commonly use authentication credentials to control access to information, applications, or other system resources. The classic combination of a user's account number or name coupled with a secret password (the *authenticator*) is a widely used example of an authentication credential. Some information systems use other forms of authenticators, such as biological characteristics (e.g., facial photo, fingerprints, voice, retinas) or public key certificates.

7.3 The PCTF Credential Model

Figure 16 illustrates the PCTF Credential Model.

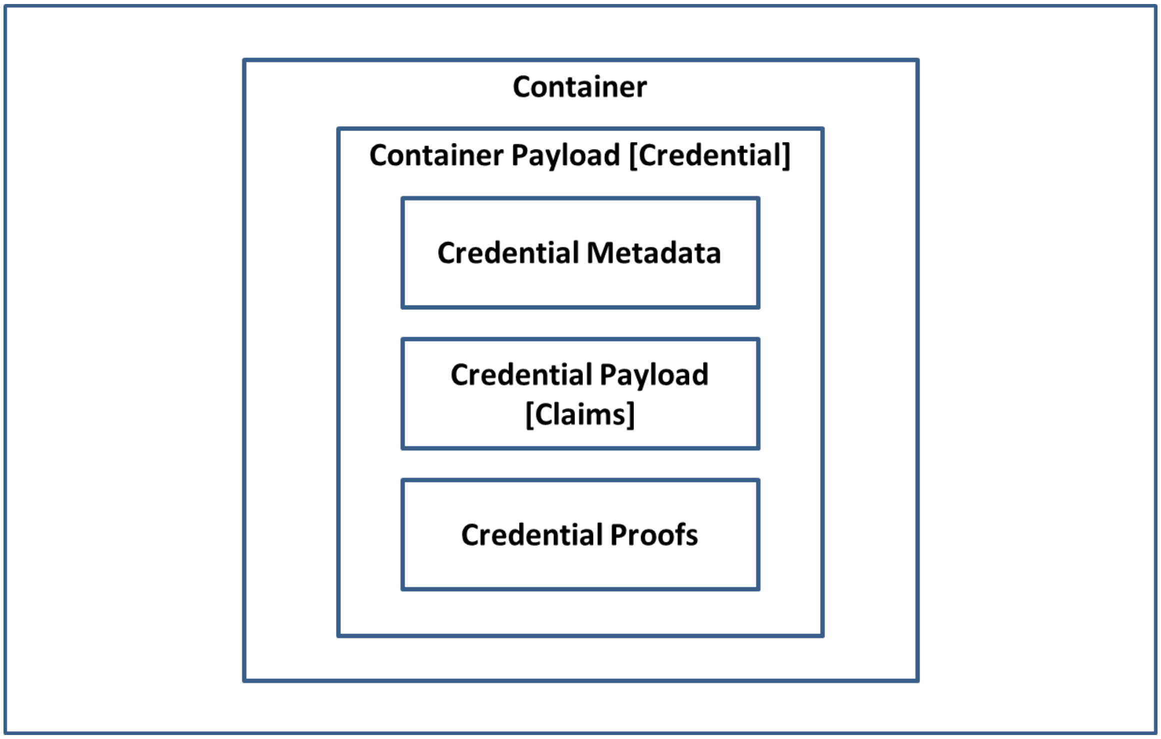


Figure 16: The PCTF Credential Model

In the PCTF Credential Model, a Credential is composed of three components:

- **Credential Metadata**: One or more *credential attributes* that describe the properties or characteristics of the Credential.
- **Credential Payload**: A set of one or more *Claims* asserted about one or more *Subjects*.
- **Credential Proofs**: One or more methods or mechanisms that are used to verify that the *Issuer* authored the Credential and that the Credential has not been tampered with.

It should be noted that although a *Verifier* can verify the authorship of a Credential and can inspect a Credential for evidence of tampering, the veracity of the Credential Payload itself cannot be verified by a Verifier (i.e., the fact of a Claim (e.g., “the sky is green”) cannot be verified). By accepting a Credential, a Verifier is essentially stating that it trusts the Issuer of the Credential to have properly ascertained the veracity of the Claims prior to creating the Credential Payload.

The *Holder* of a Credential is usually given some form of documentation as evidence of being in possession of the Credential. For many years credential documentation consisted mainly of a piece of paper or a plastic card. Over time authentication features (including electronic authentication features) were built into the plastic card. Increasingly, credentials are being issued in an electronic form[39]. The documentary evidence of a Credential can be thought of as a *container*[40] or as a substrate for transporting the Credential. The Credential is placed inside the container and becomes the *payload of the container*.

[39] The most recent specification of electronic credentials is *verifiable credentials*. See [W3C, 2021].

[40] See: [Ruff, 2020].

7.4 Claims Assertion Models

7.4.1 The Claims Assertion Model of a Subject Claim

A Subject Claim is a statement about a Subject. A Subject Claim is expressed by means of one or more *entity attributes*. Figure 17 illustrates the claims assertion model of a subject claim.

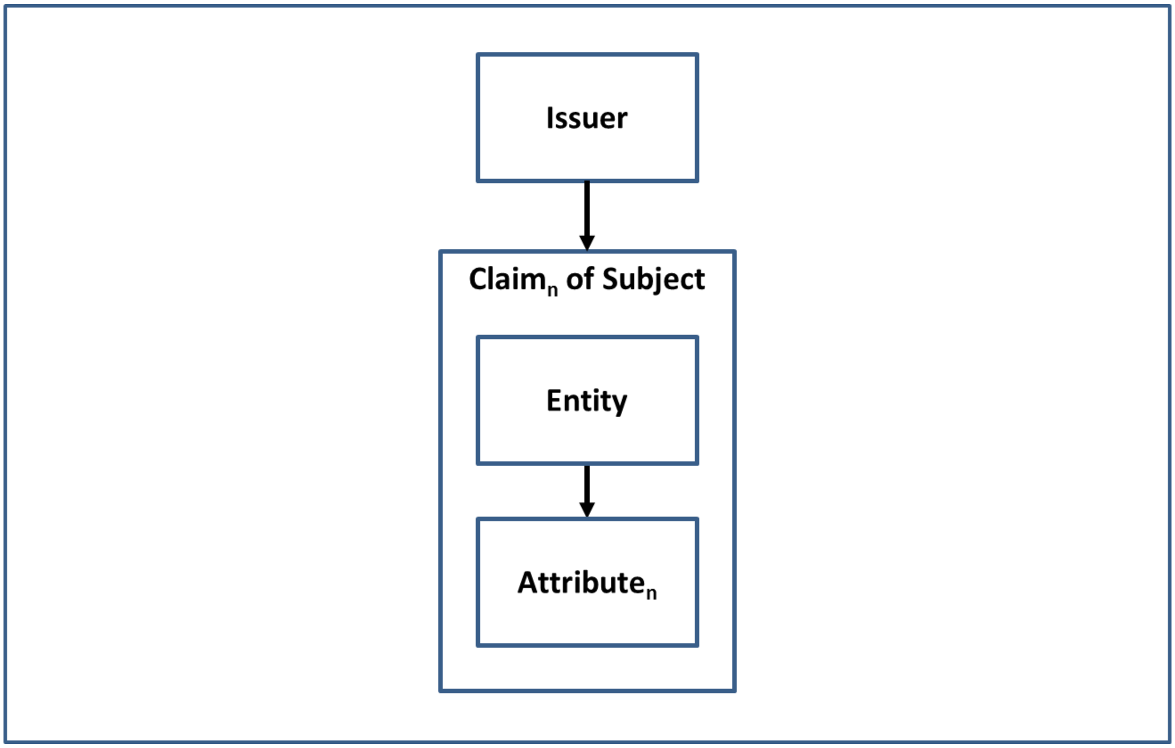


Figure 17: The Claims Assertion Model of a Subject Claim

7.4.2 The Claims Assertion Model of a Relationship Claim

A Relationship Claim is a statement about an association that exists between two or more Subjects. A Relationship Claim is expressed by means of one or more *relationship attributes*. Figure 18 illustrates the claims assertion model of a relationship claim.

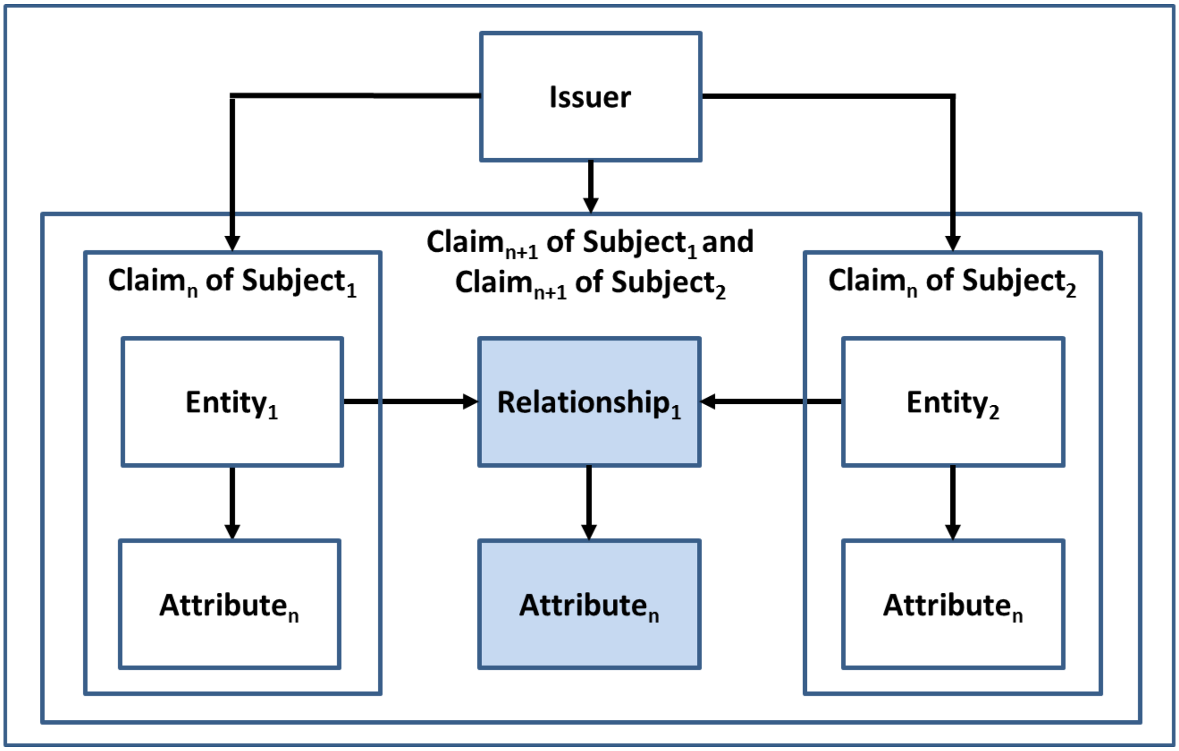


Figure 18: The Claims Assertion Model of a Relationship Claim

7.5 The Credential Issuance Model

An Issuer asserts one or more Claims about one or more Subjects, creates a Credential from these Claims, and assigns the Credential to a Holder. Figure 19 illustrates the credential issuance model.

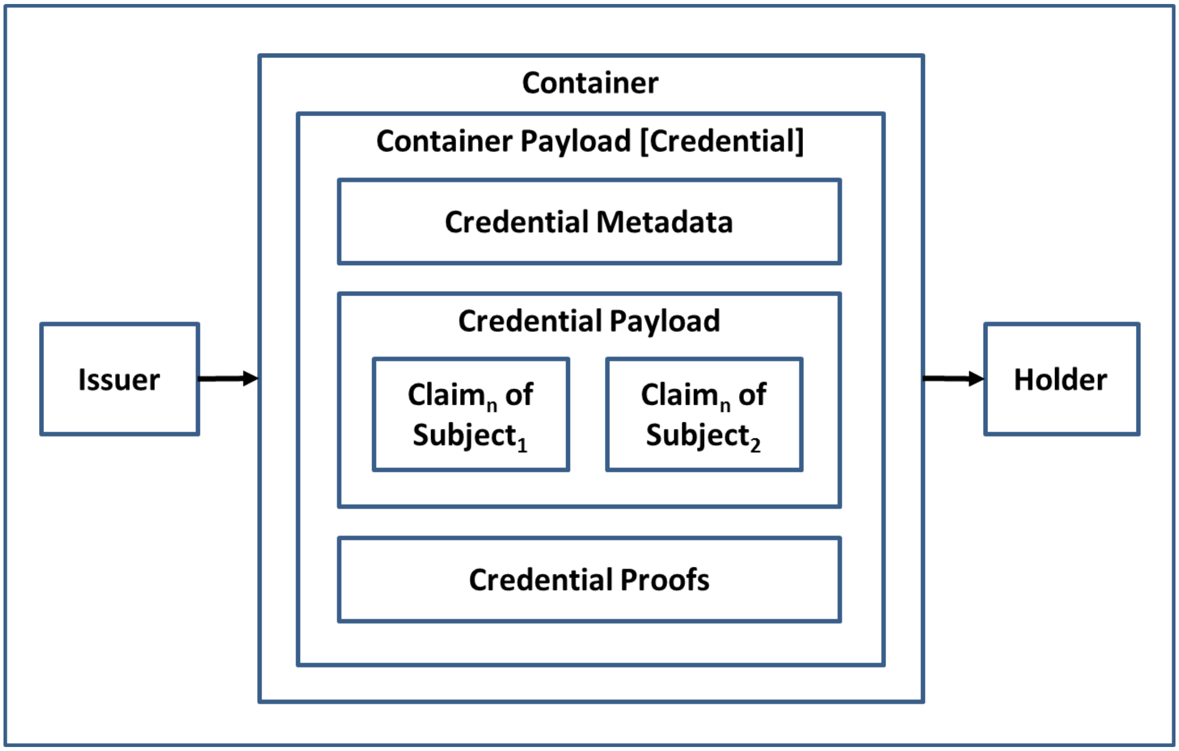


Figure 19: The Credential Issuance Model

8 APPENDIX F: IDENTITY VERIFICATION IN DETAIL

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 four 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 entity presenting the identity information is in control of the identity. Knowledge-based confirmation is achieved by means of the challenge-response model: the entity 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 entity 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 entity 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.

9 APPENDIX G: CREDENTIAL VERIFICATION IN DETAIL

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 can be used to generate a level of assurance.

The Credential Verification process is dependent on the **Credential Authenticator Binding** process (i.e., the process of associating a Credential issued to a Holder with one or more authenticators). 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 credential verifications, 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).

9.1 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 three types of authenticators:

- Something the Holder has[41] (e.g., a cryptographic key or a one-time-password).
- Something the Holder knows[42] (e.g., a password, a response to a challenge question).
- Something the Holder is or does[43] (e.g., face, fingerprints, retinas, keyboard stroke timing, gait).

The authenticators when bound to a Credential will be subsequently used to prove, with a specified level of assurance, that the Credential is referring to the same Holder that was originally bound to the Credential.

[41] This is similar to the physical possession confirmation method used by Identity Verification.

[42] This is similar to the knowledge-based confirmation method used by Identity Verification.

[43] This is similar to the biological or behavioural characteristic confirmation method used by Identity Verification.

It should be noted that given the irrevocability of biological characteristics (e.g., face, fingerprints, retinas), industry standards[44] are generally cautious in regards to the use of biological characteristics as authenticators for authentication credentials. A biological characteristic is not the same as a secret which can be changed periodically; a biological characteristic cannot be changed. Moreover, a Holder's biological characteristic can be replicated. For example, a threat actor may obtain a copy of the Holder's fingerprint, construct a replica, and pass credential verification (assuming that the credential verification process does not block such attacks by employing robust liveness detection techniques).

However, a biological characteristic may be used to unlock access to an authenticator stored within a local device in order to facilitate remote credential verification with a service. An example of such a scenario is the use of facial recognition software to unlock access to a mobile one-time passcode or other locally stored and generated mobile authenticator.

[44] For examples, see NIST 800-63 and ITSP.30.031.

10 APPENDIX H: 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.

10.1 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.

10.2 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.

10.3 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.

10.4 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.

11 APPENDIX I: THEMATIC ISSUES

The PSP PCTF Working Group has identified several high-level thematic issues that must be addressed in order to advance the digital ecosystem.

Thematic Issue 1: Relationships (Priority: High)

The development of a relationship model is required.

Status: Completed.

Thematic Issue 2: Credentials (Priority: High)

The development of a generalized credential model is required. This model should integrate traditional physical credentials and authentication credentials with the broader notion of a verifiable credential.

Status: Completed.

Thematic Issue 3: Unregistered Organizations (Priority: High)

Currently, the scope of PSP 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 needs to be undertaken.

Thematic Issue 4: Informed Consent (Priority: High)

The current version of the PSP PCTF Consolidated Overview document may not adequately capture all the issues and nuances surrounding the topic of informed consent especially in the context of the public sector. A more rigorous exploration of this topic needs to be done.

Thematic Issue 5: Privacy Concerns (Priority: Medium)

In regards to the *Identity Continuity* and *Relationship Continuity* atomic processes, it has been noted that there are privacy concerns with the notion of *dynamic confirmation*. Further analysis based on feedback from the application of the PSP PCTF is required to determine if these atomic processes are appropriate.

Thematic Issue 6: Assessing Outsourced Atomic Processes (Priority: Medium)

The PSP PCTF does not assume that a single Issuer or Verifier is solely responsible for all of the atomic processes. An organization may choose to outsource or delegate the responsibility of an atomic process to another party. Therefore, several bodies might be involved in the PSP PCTF assessment process, focusing on different atomic processes, or different aspects (e.g., security, privacy, service delivery). It remains to be determined how such multi-actor assessments will be conducted.

Thematic Issue 7: Scope of the PSP PCTF (Priority: Low)

It has been suggested that the scope of the PSP PCTF should be broadened to include other domains such as academic qualifications, professional designations, vaccination status, etc. The PSP PCTF anticipates extensibility through the generalization of the PSP PCTF model and the potential addition of new atomic processes. Expanding the scope of the PSP PCTF into other domains needs to be studied.

Thematic Issue 8: Signature (Priority: Low)

The concept of signature as it is to be applied in the context of the PSP PCTF needs to be explored.

Thematic Issue 9: Foundation Name, Primary Name, Legal Name (Priority: Low)

The PSP PCTF has definitions for *Foundation Name*, *Primary Name*, and *Legal Name*. Since the three terms mean the same thing, a preferred term should be selected and used consistently throughout the PSP PCTF documents.

Thematic Issue 10: Additional Detail (Priority: Low)

It has been noted that the PSP PCTF Consolidated Overview document contains insufficient detail in regards to the specific application of the PSP PCTF. The PSP PCTF Consolidated Overview document needs to be supplemented with detailed guidance in a separate document.

Thematic Issue 11: Review of the Appendices (Priority: Low)

A review of the current appendices contained in the PSP PCTF Consolidated Overview document needs to be undertaken. Each appendix should be evaluated for its utility, applicability, and appropriateness, and a determination made as to whether it should continue to be included in the document.

12 APPENDIX J: 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)
    g. Credentials (Relationships & Attributes) Component Overview (July 2020)
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 (Editor's Draft) (2021)

Individuals

1. Joe Andrieu
    a. A Primer on Functional Identity (2018)
2. Timothy Ruff
    a. Verifiable Credentials Aren't Credentials. They're Containers (2020)