



CAN/DGSI 103-0:202X
NATIONAL STANDARD OF CANADA

First Edition
202X-XX

Digital trust and identity – Part 0: Techniques – Code of Practice

35.020



- Page left intentionally blank -

Table of Contents

Foreword.....	vi
Introduction	viii
Digital trust and identity – Part 0: Techniques – Code of Practice.....	1
1 Scope.....	1
2 Normative References	1
3 Terms and Definitions.....	1
4 Overview	18
4.1 The Identity Management Ecosystem in Canada.....	18
4.2 The Pan-Canadian Trust Framework (PCTF).....	19
4.3 The PCTF Model	20
5 Normative Core	22
5.1 Digital Representations: General	22
5.2 Digital Representations: Entities.....	22
5.3 Digital Representations: Relationship between entities.....	23
5.4 Digital Representations: Attributes.....	25
5.5 Identity types	26
5.6 Atomic and compound processes	27
5.7 Dependencies.....	31
5.8 Conformance Criteria.....	31
5.9 Qualifiers.....	31
6 Mutual Recognition	32
6.1 Mutual Recognition General	32
6.2 Process Mapping.....	32
6.3 Alignment to other frameworks	34
6.4 Assessment	34
6.5 Acceptance.....	35
7 Supporting infrastructure	36
7.1 Supporting Infrastructure General.....	36
7.2 Methods.....	36
7.3 Conveyance Mechanisms.....	37

8	Digital ecosystem roles and information flows.....	39
8.1	Roles.....	39
8.2	Information Flows.....	40
9	Atomic processes in detail	41
9.1	Identity Domain Processes.....	41
9.2	Relationship Domain Processes	44
9.3	Credential Domain Processes.....	47
9.4	Consent Domain Processes	49
9.5	Signature Domain Processes.....	51
10	Qualifiers in detail	52
10.1	Identity Domain Qualifiers	52
10.2	Pan-Canadian Levels of Assurance (LOA) Qualifiers.....	52
10.3	Signature Domain Qualifiers	54
10.4	Other Trust Framework Qualifiers	54
	Annex A: Identity Management Overview	55
	A.1 Identity	55
	A.2 Defining the Population.....	55
	A.3 Defining the Identity Context.....	56
	A.4 Determining Identity Information Requirements.....	56
	A.5 Identity Resolution	59
	A.6 Ensuring the Accuracy of Identity Information	59
	Annex B: Legal Entities.....	61
	B.1 Types of Legal Entities.....	61
	B.2 Treatment of Legal Entity Information.....	61
	Annex C: Relationships in Detail	62
	C.1 Relationship Models	62
	C.2 Relationships within an Organization.....	63
	C.3 Organization to Organization Relationships	64
	Annex D: Credentials Overview	66
	D.1 What is a Credential?.....	66
	D.2 Types of Credentials	66

D.3 Information Contained in a Credential	67
D.4 Documentation of a Credential	69
D.5 The PCTF Credential Model	69
D.6 PCTF Claims Assertion Models	71
D.7 The PCTF Credential Issuance Model	72
Annex E: Identity Verification in Detail	74
Annex F: Credential Verification in Detail	75
F.1 Authenticators	75
Annex G: Guidelines on Mutual Recognition	77
G.1 Planning and Engagement	77
G.2 Process Mapping	78
G.3 Assessment	78
G.4 Acceptance	79
Annex H: Thematic Issues	80
Bibliography	82

Foreword

The Digital Governance Standards Institute (DGSI) develops digital technology governance standards fit for global use. The Institute works with experts, as well as national and global partners and the public to develop national standards that reduce risk to Canadians and Canadian organizations adopting and using innovative digital technologies in today's digital economy.

DGSI standards are developed in accordance with the *Requirements & Guidance – Accreditation of Standards Development Organizations*, 2019-06-13, established by the Standards Council of Canada (SCC).

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. DGSI shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of this Standard are included in the Introduction.

For further information about DGSI, please contact:

Digital Governance Standards Institute

500-1000 Innovation Dr.

Ottawa, ON K2K 3E7

www.dgc-cgn.org

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

- Page left intentionally blank -

Introduction

This is the First Edition of CAN/DGSI 103-0:202X, Digital trust and identity – Part 0: Techniques – Code of Practice.

CAN/DGSI 103-0:202X was prepared by the Digital Governance Standards Institute Technical Committee 4 (TC 4) on digital trust and identity, comprised of over 160 thought leaders and experts in identity management and related subjects. This Standard was approved by a Technical Committee formed balloting group, comprised of X producers, X government / regulator / policymakers, X users, and X general interests.

This Standard is based on the Public Sector Profile of the Pan-Canadian Trust Framework (PSP-PCTF) version 1.5 (October 2024) licensed under the Open Government Licence – Canada. The PSP-PCTF may be found at: <https://github.com/canada-ca/PCTF-CCP>. Terms of the Open Government License may be found at: <https://open.canada.ca/en/open-government-licence-canada>

All units of measurement expressed in this Standard are in SI units using the International system (SI).

This Standard is subject to technical committee review beginning no later than one year from the date of publication. The completion of the review may result in a new edition, revision, reaffirmation or withdrawal of the Standard.

The intended primary application of this Standard is stated in its scope. It is important to note that it remains the responsibility of the user of the Standard to judge its suitability for a particular application. This Standard is intended to be technology agnostic.

This Standard is not intended to be used for conformity assessment.

ICS 35.020

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE

- Page left intentionally blank -

Digital trust and identity – Part 0: Techniques – Code of Practice

1 Scope

This document provides a reference set of generic digital trust, identity, credentials, and wallets techniques including implementation guidance.

This document is designed to be used by organizations:

- a) within the context of a digital trust and identity management system based on the CAN/DGSI 103 series of standards;
- b) for implementing digital trust and identity programs based on internationally recognized best practices; and
- c) for developing organization-specific digital trust and identity guidelines.

This document applies to all organizations, including public and private companies, government entities, and not-for-profit organizations.

2 Normative References

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

CAN/DGSI 103-1:2023, Digital Trust and Identity – Part 1: Fundamentals

CAN/DGSI 103-3:2024, Digital Trust and Identity – Part 3: Digital credential management system

3 Terms and Definitions

For the purposes of this document, the following terms and definitions shall apply. If a definition that follows conflicts with a definition in CAN/DGSI 103-1 then the definition in CAN/DGSI 103-1 shall apply.

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 "Relationship", "Balanced Relationship", and "Directed Relationship".

agent

An Entity that acts on behalf of another 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”.

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,
© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

corporations in a joint venture). See also “Relationship”, “Agency Relationship”, and “Directed 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 Subject 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 Subject 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.

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. 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 Organizations (public and private sector). Internal clients are generally employees and contractors.

compound entity

An Entity that is comprised of one or more Atomic Entities and/or one or more subordinate Compound 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

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

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; to which parties the personal information is being disclosed (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; under whose jurisdiction or authority the consent notice statement is issued; and the rights of and process to revoke any consent given in whole or in part pursuant to such consent notice. 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, the identity information of 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 or revocation 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.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

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, driver licensing, or social media). Depending on the identity context, a contextual identity may be tied to a foundational identity (e.g., a driver’s licence) or may not be tied to a foundational identity (e.g., a social media profile). See also “foundational identity”.

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.

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 verification attempts, © DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

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 about one or more Subjects 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, that the Credential has not been tampered with, and that the Credential has been bound to a Holder.

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.

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 credential

A Credential that has been issued in a digital form. See also “Credential”.

digital ecosystem

A collection of various tools and systems, and the actors who create, interact with, use, and remake them.

digital entity

An electronic representation of an Entity that is exclusive to the Entity.

digital relationship

An electronic representation of an association between two or more Entities.

digital representation

An electronic representation of an Entity or an electronic representation of an association between two or more Entities.

digital signature

A cryptographic scheme for verifying the authorship of a digital message or document and for verifying that the digital message or document was not altered in transit (i.e., tampered with). A digital signature can also provide a means for non-repudiation (i.e., the author cannot successfully claim that they did not sign the digital message or document).

directed relationship

A Relationship where the Entities are not equals (e.g., parent and child, parent corporation and

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

subsidiary corporation, manager and subordinate). See also “Relationship”, “Agency Relationship”, and “Balanced Relationship”.

eIDAS

Electronic Identification, Authentication, and Trust Services (eIDAS) is a European Union regulation that oversees electronic identification and trust services for electronic transactions in the European Union's internal market. It regulates electronic signatures, electronic transactions, involved bodies, and their embedding processes to provide a safe way for users to conduct business online such as electronic funds transfer or transactions with public services.

electronic or digital evidence

Any data that is recorded or preserved on any medium in, or by, a computer system or other similar device. Examples include database records, audit logs, and electronic word processing documents.

entity

A thing with a distinct and independent existence, such as a person 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.

entity information

Information about an identifiable Entity.

evidence of contextual identity (of an organization)

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 contextual identity (of a person)

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, © DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

drive, or obtain health services; and records of marriage, name change, or death originating from a jurisdictional authority.

evidence of foundational identity (of an organization)

Evidence of identity that establishes core identity information about an organization such as legal name, date of foundational event, address, status, and primary contact. Examples are registration records, certificates of compliance, and incorporation records from an authority with the necessary jurisdiction.

evidence of foundational identity (of a person)

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

A record from an authoritative source indicating an Entity's identity. There are two categories of evidence of identity: evidence of foundational identity and evidence of contextual identity.

See "evidence of foundational identity" and "evidence of contextual identity".

FATF

The 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

The 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 an Entity as indicated on an official record identifying the Entity (e.g., provincial/territorial vital statistics record, federal immigration record, provincial/territorial business registry record, federal corporate registry record).

foundation registry (of organizations)

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

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]).

foundation registry (of persons)

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]).

foundational event

A significant discrete episode that occurs in the life span of a person or an organization. By law a foundational event must be recorded with a government entity and is subject to legislation and regulation. Examples of foundational events for persons 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. Examples of foundational events for organizations are registration of charter, merger, amalgamation, surrender of charter, and dissolution.

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). See also “contextual identity”.

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.

NOTE: If the Holder is not the Subject of a Credential, then the Holder must have the legal status to represent the Subject (e.g., a legal guardian, or an attorney).

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 within a population. 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 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 population.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

identity evidence acceptance

The process of confirming that the evidence of identity presented (whether physical or electronic) is acceptable.

identity evidence determination

The process of determining the acceptable evidence of identity (whether physical or electronic).

identity information

The set of identity attributes that is sufficient to distinguish one Entity from all other Entities within a population.

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 foundational event, a change in their identity information, or an indication that their identity information has been exposed to a risk factor (e.g., the death of the person, a charter surrender, use of expired documents, a privacy breach, fraudulent use of the identity information).

identity information retrieval

The disclosure of identity information about 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.

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

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 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 information or shared secrets to prove that the Subject presenting the identity information is in control of the identity. Knowledge-based confirmation is achieved by means of the challenge-response model: the Subject 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).

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

The 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 (e.g., a Credential) to prove that the Subject 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
© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

by different Issuers.

presentation confirmation

A determination by the Verifier of the correctness of the Presentation.

primary name

The name that an Entity uses for formal and legal purposes (also known as “legal name”). See also “foundation name”.

relationship

An association between two or more Entities. See also “Agency Relationship”, “Balanced Relationship”, and “Directed Relationship”.

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 acceptance

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

The process of confirming that the evidence of a Relationship presented (whether physical or electronic) is acceptable.

relationship evidence determination

The process of determining the acceptable evidence of a Relationship (whether physical or electronic).

relationship identifier

The set of identifiers of the Entities 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 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 within a 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

© DGSI 2024 – All rights reserved. Unauthorized reproduction is strictly prohibited.

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.

shall

A requirement.

should

A recommendation.

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 a 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.

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 Subject 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

The United Nations Commission on International Trade Law (UNCITRAL) is mandated 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.

verifiable credential

A digitally signed Digital Credential. Specifically, a Digital Credential that conforms to the Verifiable Credentials Data Model of the World Wide Web Consortium (W3C). See also “digital signature”.

4 Overview**4.1 The Identity Management Ecosystem in Canada**

- 4.1.1 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 identity management ecosystem employs a federated identity model.

4.2 The Pan-Canadian Trust Framework (PCTF)

- 4.2.1 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. 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.
- 4.2.2 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.
- 4.2.3 The PCTF enables the alignment and assessment of business processes, thereby increasing confidence in identity and credential 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 or a credential solution and identifies any dependencies on external organizations.
- 4.2.4 The PCTF enables the recognition and acceptance of:
- Digital Entities; and
 - Digital Relationships between Entities.
- 4.2.5 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.
- 4.2.6 The PCTF is designed to take into consideration international 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).
- 4.2.7 The PCTF is not a governance framework.
- 4.2.8 Currently, the scope of the Pan-Canadian Trust Framework is:
- Persons in Canada: all citizens and legal 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.

4.3 The PCTF Model

4.3.1 The PCTF model consists of four main components:

1. The **Normative Core** component that encapsulates the key concepts of the PCTF;
2. The **Mutual Recognition** component that outlines the current methodology that is used to assess and certify actors in the digital ecosystem;
3. The **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. The **Digital Ecosystem Roles and Information Flows** component that defines the roles and information flows within the digital ecosystem.

4.3.2 All items in the Normative Core component are prescriptive. The Mutual Recognition component describes a recommended methodology for conducting a program assessment, but it is not mandatory that the methodology be followed. The contents found in the Supporting Infrastructure and Digital Ecosystem Roles and Information Flows components are descriptive only and are not prescriptive.

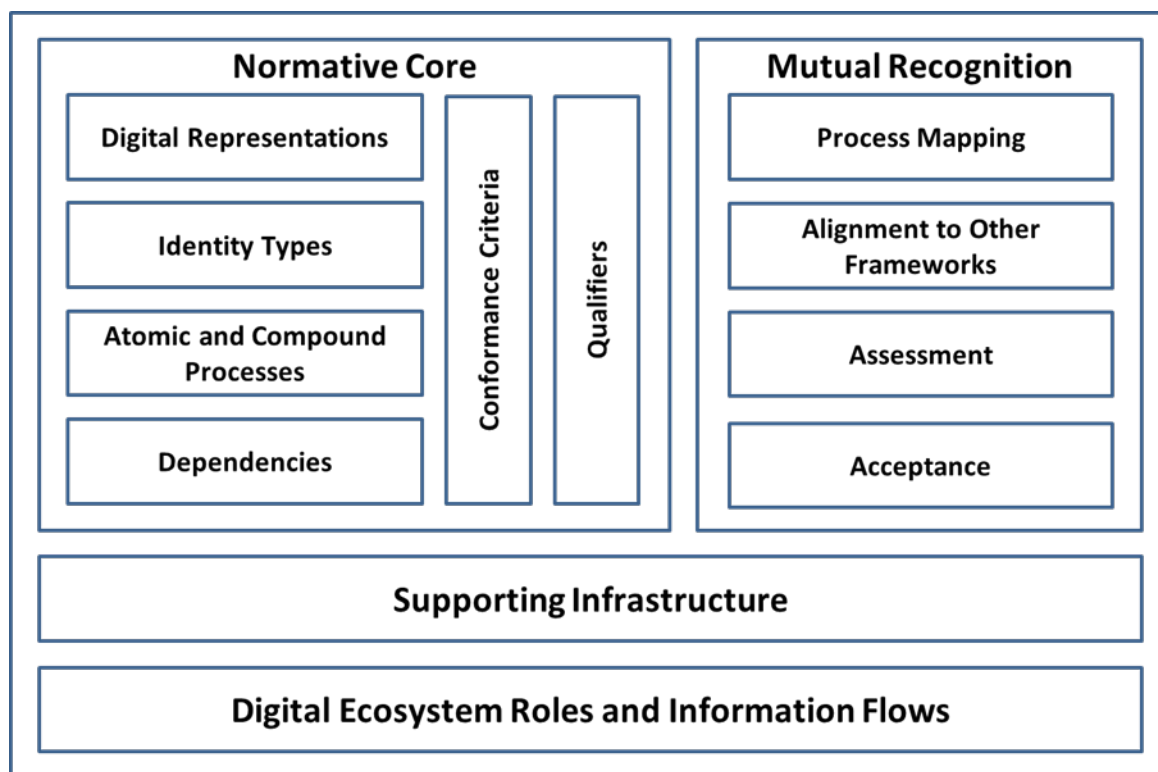


Figure 1: The Pan-Canadian Trust Framework Model

5 Normative Core

5.1 Digital Representations: General

- 5.1.1 A **Digital Representation** is an electronic representation of an **Entity** or an electronic representation of an association between two or more Entities. Digital Representations are intended to model real-world Entities, such as persons and organizations.
- 5.1.2 Currently, the PCTF recognizes two types of Digital Representations:
 - 1. **Digital Entity**: An electronic representation of an Entity that is exclusive to the Entity.
 - 2. **Digital Relationship**: An electronic representation of an association between two or more Entities.
- 5.1.3 A Digital Representation is the final output of a set of processes and therefore can be conceptualized as a set of state transitions.
- 5.1.4 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.

5.2 Digital Representations: Entities

- 5.2.1 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.
- 5.2.2 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 and/or one or more subordinate Compound Entities. Organizations are Compound Entities. In its simplest form, a Compound Entity is comprised of one or more Atomic Entities. However, it may also be the case that a Compound Entity is composed of one or more subordinate Compound Entities. An even more complex Compound Entity may be comprised of one or more independent Atomic Entities along with one or more subordinate Compound Entities. Figure 2 illustrates the two types of Entities.

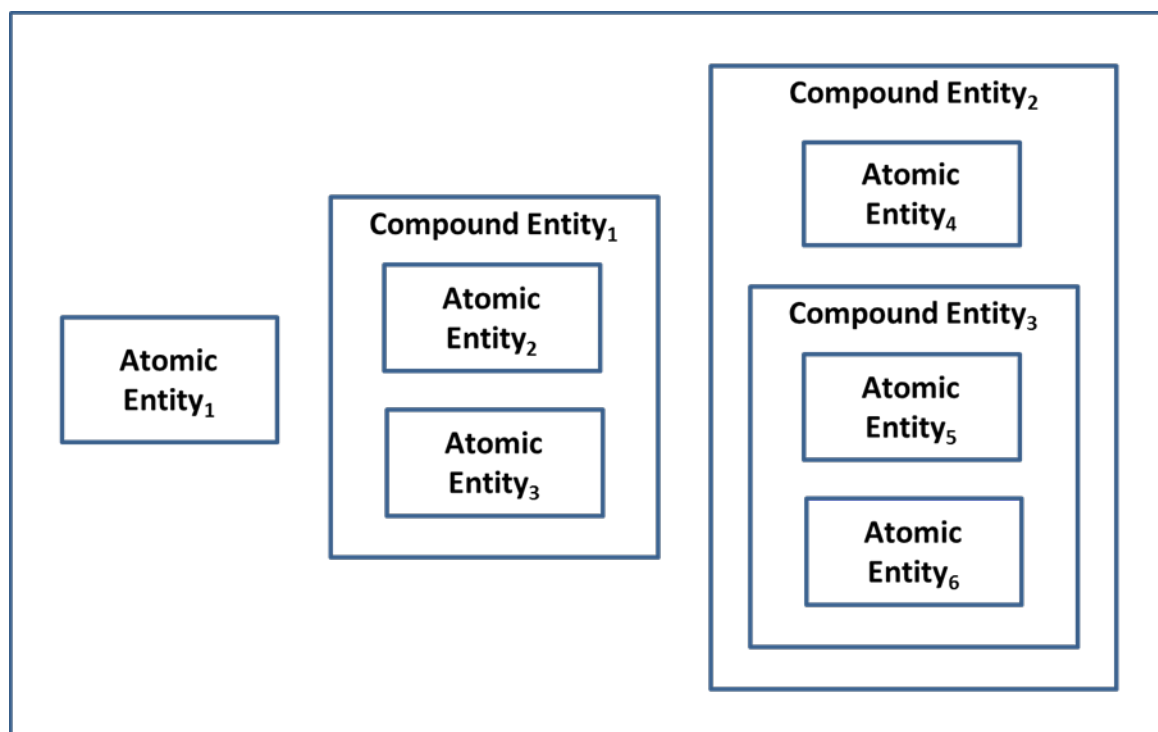


Figure 2: Atomic Entities and Compound Entities

5.3 Digital Representations: Relationship between entities

- 5.3.1 A **Relationship** is an association between two or more Entities. The Entities in the Relationship can be any combination of Atomic Entities and Compound Entities. 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)
- 5.3.2 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.
- 5.3.3 Figure 4 shows a view of a Relationship between two Compound Entities. Note that one of the Compound Entities has an internal Relationship between two Atomic Entities.

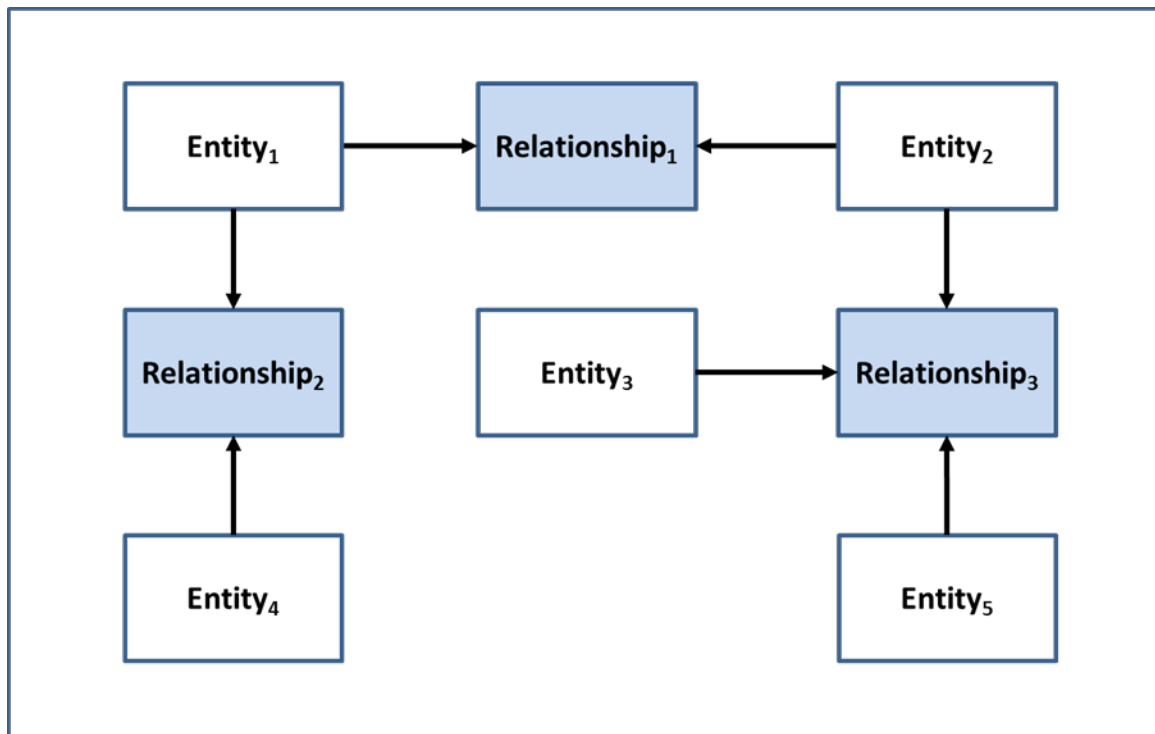


Figure 3: A Network of Entities and Relationships

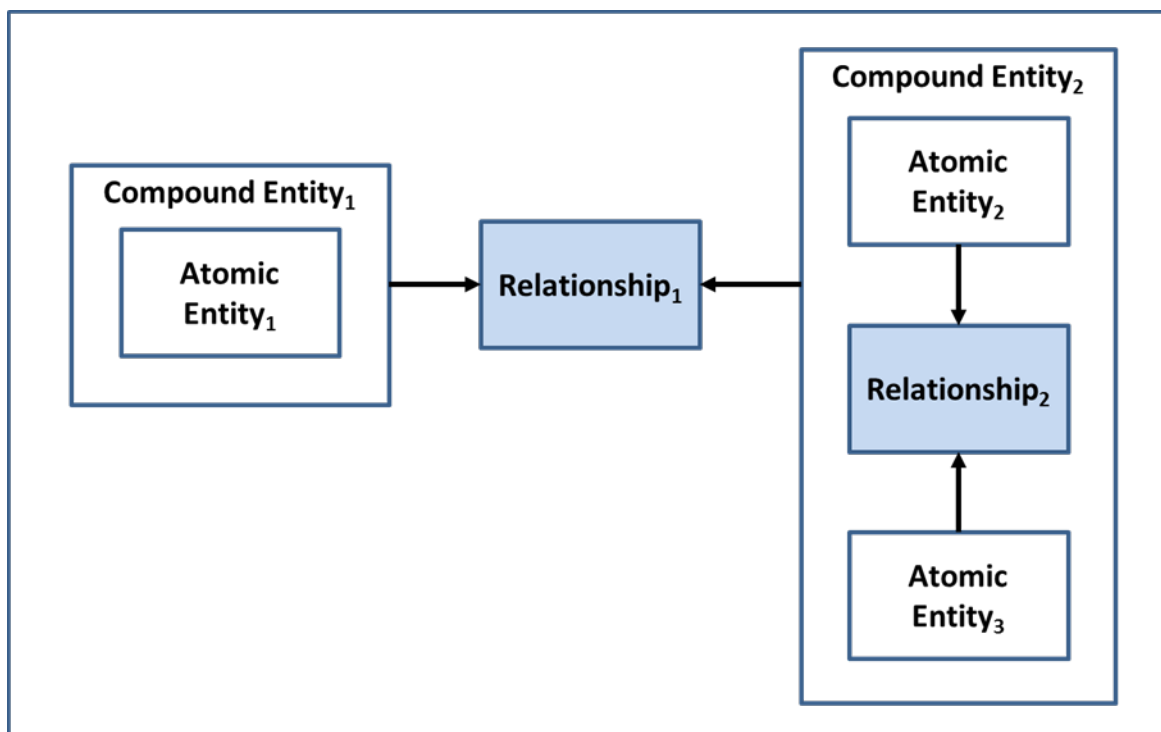


Figure 4: A Relationship between Two Compound Entities

5.4 Digital Representations: Attributes

- 5.4.1 An **Attribute** is defined as a property or characteristic of a thing. The PCTF recognizes three types of Attributes: Entity Attributes, Relationship Attributes, and Credential Attributes. Entity Attributes and Relationship Attributes are used to express Claims.
- 5.4.2 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
- 5.4.3 A **Relationship Attribute** is a property or characteristic of an association between two or more 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 of the Relationship
 - The effective date of the Relationship
 - The expiry date of the Relationship
 - The status of the Relationship (e.g., active, revoked)

5.4.4 A **Credential Attribute** is a property or characteristic of a Credential. Credential Attributes are also known as **Credential Metadata**. Some examples of Credential Attributes include:

- The identifier that uniquely identifies the instance of the Credential (e.g., a document identifier, a passport number, a birth certificate number, a banking credential identifier)
- The type of Credential
- The Issuer of the Credential
- The issuance date of the Credential
- The expiry date of the Credential
- The status of the Credential (e.g., active, suspended, revoked)

5.5 Identity types

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

5.5.2 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).

5.5.3 A **Contextual Identity** is an identity that is used for a specific purpose within a specific identity context (e.g., banking, business permits, health services, driver licensing, or social media). Depending on the identity context, a contextual identity may be tied to a foundational identity (e.g., a driver's licence) or may not be tied to a foundational identity (e.g., a social media profile).

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

For Persons

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

- temporary residents in Canada
- refugee claimants
- foreign-born visitors

For Organizations

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

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

5.6 Atomic and compound processes

5.6.1 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. A state transition is the transformation of an object input state to an output state. 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.

5.6.2 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. The digital ecosystem is intended to interoperate seamlessly across different organizations, sectors, and jurisdictions, and to be interoperable with other trust frameworks.

NOTE: While most atomic processes are employed many times by a program/service, four atomic processes – Identity Information Determination, Identity Evidence Determination, Relationship Information Determination, and Relationship Evidence Determination – are carried out only once for a program/service.

5.6.3 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.

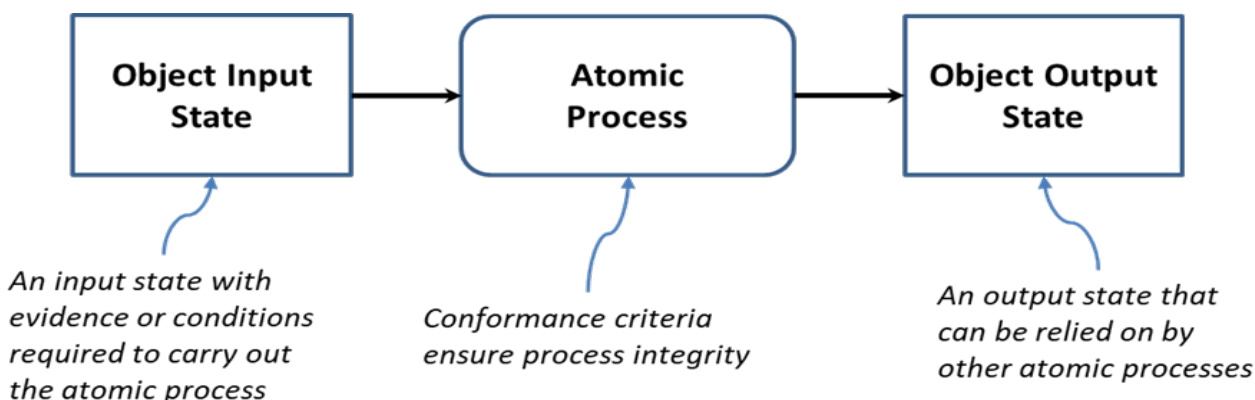


Figure 1: The Atomic Process Model

- 5.6.4 Atomic processes are crucial building blocks to ensuring the overall integrity of the digital supply chain and therefore, the integrity of digital services. The integrity of an atomic process is paramount because the output of an atomic process is relied upon by many participants – across jurisdictional and public and private sector boundaries, and over the short term and the long term. The PCTF ensures the integrity of an atomic process through a set of well-defined conformance criteria that support an impartial, transparent, and evidence-based assessment and certification process.
- 5.6.5 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.

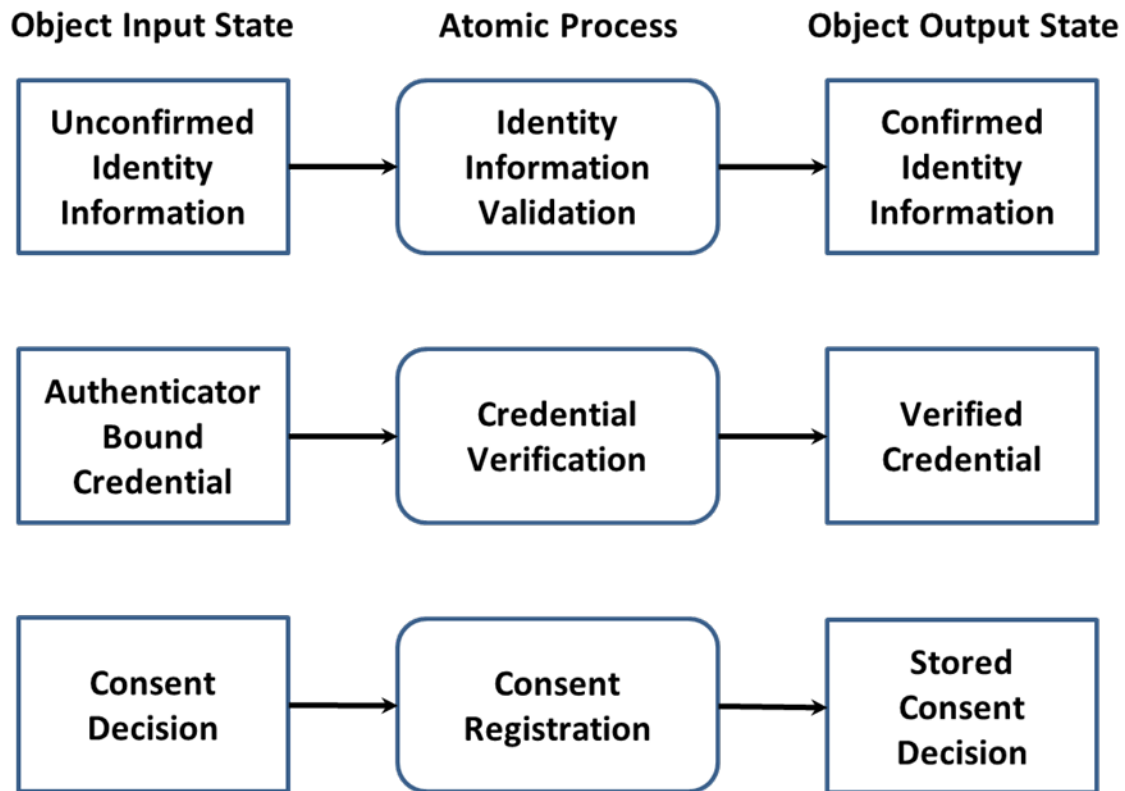


Figure 2: Examples of Atomic Processes (Modeled)

- 5.6.6 The primary function of the PCTF is to assess and certify business processes. When analyzed, business processes are often composed of several atomic processes. A set of atomic processes grouped together form a compound process that results in a set of state transitions. It may also be the case that a compound process is composed of a set of other compound processes which in turn can be decomposed into a set of atomic processes.
- 5.6.7 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. Note that different parties may use different terms for compound processes that are functionally the same (or similar). For example, another party may refer to the set of 5 atomic processes shown in Figure 7 as Identity Proofing.

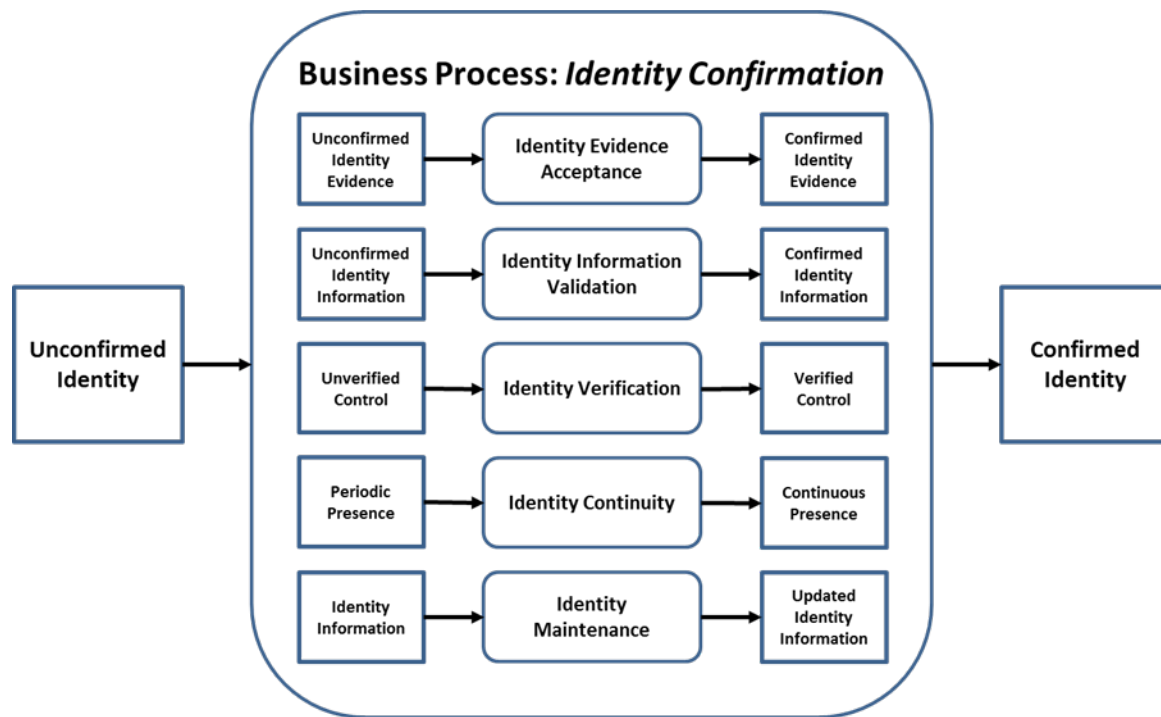


Figure 7: Example of a Compound Process (Modeled)

5.7 Dependencies

- 5.7.1 The PCTF recognizes two types of dependencies. The first type of dependency is a dependency that exists between two or more atomic processes. Although each atomic process is functionally discrete, to produce an acceptable output an atomic process may require the successful prior execution of another atomic process. For example, although Identity Establishment of an Entity can be performed independently at any time, it is logically correct to do so only after Identity Resolution for that Entity has been achieved. This type of dependency is specified in the conformance criteria.
- 5.7.2 The second type of dependency is a dependency on an external organization (e.g., a credential service provider) for the provision of one or more atomic process outputs. This type of dependency is identified and noted in the assessment process.

5.8 Conformance Criteria

- 5.8.1 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.
- 5.8.2 For example, the Identity Resolution atomic process usually involves assigning an identifier to an Entity. The conformance criteria specify that the atomic process must ensure that the identifier that is assigned to the Entity is unique for a specified population.
- 5.8.3 The conformance criteria are maintained in a separate document – the PCTF Assessment Workbook.

5.9 Qualifiers

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

- 5.9.2 Qualifiers can also be used to map conformance criteria to jurisdictional policy or regulatory requirements. For example, the conformance criteria for the Identity Verification atomic process that have a Pan-Canadian Level of Assurance Qualifier value of “IP1” can be mapped to Identity Assurance Level 1 as defined in the Standard on Identity and Credential Assurance issued by the Treasury Board Secretariat of Canada. In addition, qualifiers can be used to facilitate the mapping of conformance criteria equivalencies across different trust frameworks.
- 5.9.3 A conformance criterion may have a single qualifier value (i.e., the conformance criterion is applicable in only a certain case), or several qualifier values (i.e., the conformance criterion is applicable in several cases). Consult the PCTF Assessment Workbook (a separate document) for examples of how qualifiers and their values are used for assessment and how they may be mapped to other frameworks.

6 Mutual Recognition

6.1 Mutual Recognition General

- 6.1.1 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.
- 6.1.2 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.

6.2 Process Mapping

- 6.2.1 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.
- 6.2.2 In most cases, this mapping is applied to an existing program/service currently in operation, but it may also be used as an aid in the design of a new program/service. The table below gives some examples of mapping atomic processes to business processes.

Atomic Process	Business Process Examples
Identity Resolution	A service enrolment process that attempts to uniquely identify a person based on the person’s full name and date of birth

Atomic Process	Business Process Examples
	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 creates 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 Verification	Asking questions of the person presenting the identity information – 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
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

6.3 Alignment to other frameworks

- 6.3.1 Alignment of processes, systems, and solutions assists in mutual recognition across an international context where multiple frameworks may be in use.
- 6.3.2 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
- 6.3.3 Although International mutual recognition is still in its early phases, consideration should be given to aligning to these frameworks before commencing the assessment process.

6.4 Assessment

- 6.4.1 The PCTF defines a set of atomic processes and accompanying conformance criteria. Once the business processes have been mapped to the atomic processes, the business processes can be assessed, and a determination made against the related atomic process conformance criteria.
- 6.4.2 The 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 business processes and to assist the assessment team in cross-referencing data for assessment analysis. Qualifiers assigned to the conformance criteria assist in the selection of the conformance criteria that are applicable to the assessment process.
- 6.4.3 Evidence collected to support the analysis and substantiate the determination should be recorded in a manner that can be easily cross-referenced to the applicable conformance criteria.

- 6.4.4 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 parties that might need to work together to yield an overall PCTF assessment. The organization under assessment is accountable for all parties within the scope of the assessment. The assessment will note those cases where the organization under assessment feels that such general accountability is not feasible.
- 6.4.5 As the PCTF assessment process evolves, consideration will be given to determine which recognized standards are best suited to meet stakeholder requirements and best applied in relation to the PCTF.

6.5 Acceptance

- 6.5.1 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.
- 6.5.2 Eventually, the PCTF acceptance process may include standard processes defined by the International Organization for Standardization (ISO) as follows:
- Certification: The provision by an independent body (the certification 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 (the accreditation body) that a certification body operates according to international standards.
- 6.5.3 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.

7 Supporting infrastructure

7.1 Supporting Infrastructure General

- 7.1.1 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 and standards 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.

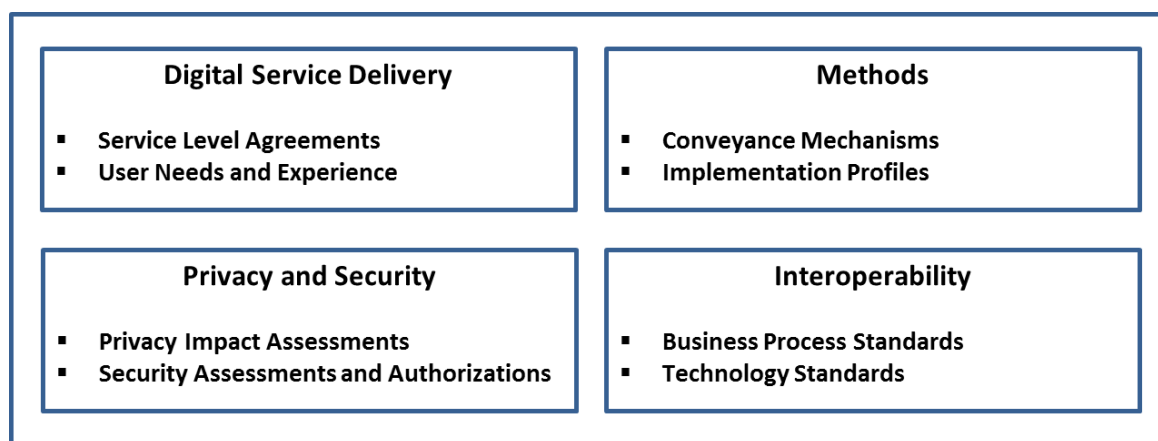


Figure 8: Supporting Infrastructure

7.2 Methods

- 7.2.1 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, 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.

NOTE: The PCTF does not recommend one Method over another.

7.3 Conveyance Mechanisms

7.3.1 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.

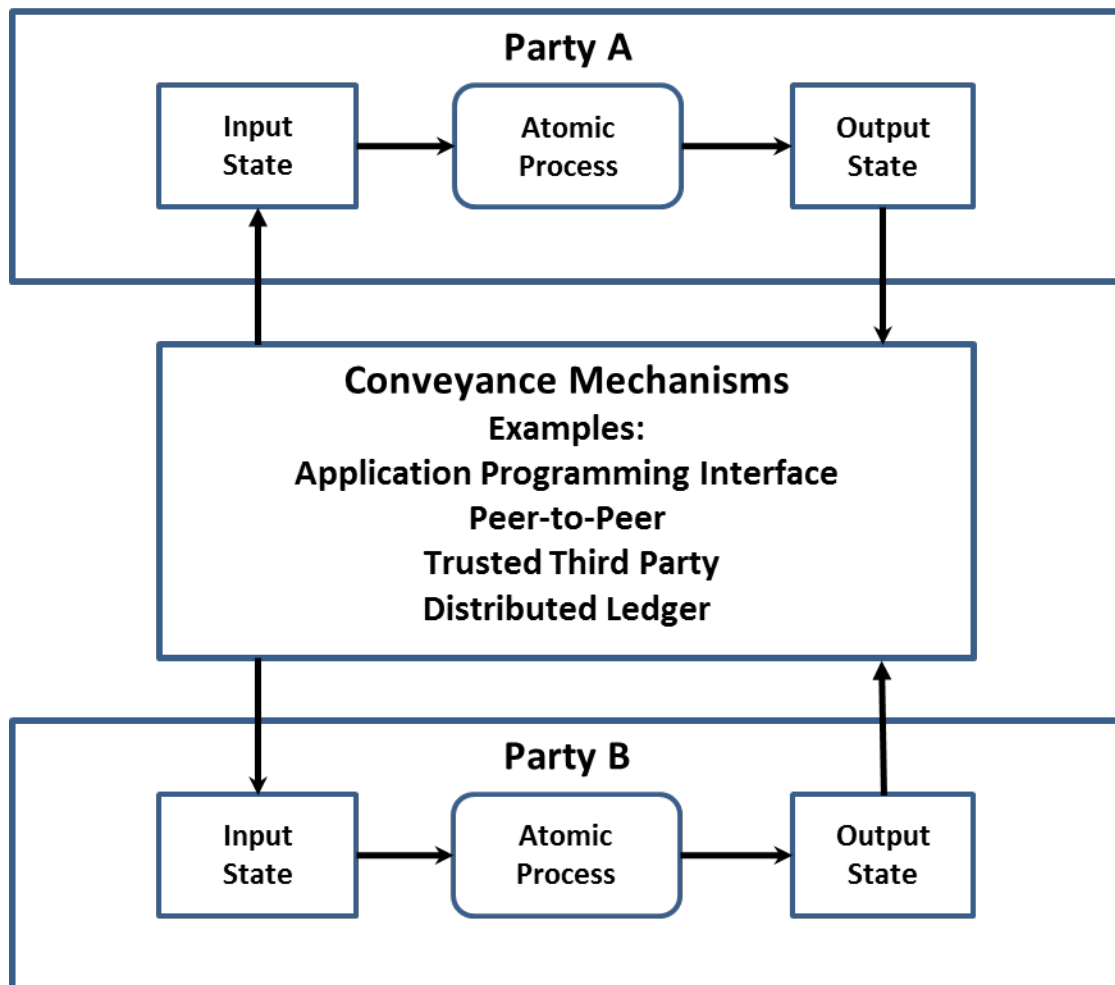


Figure 9: Conveying Output States between Parties

NOTE: 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.

8 Digital ecosystem roles and information flows

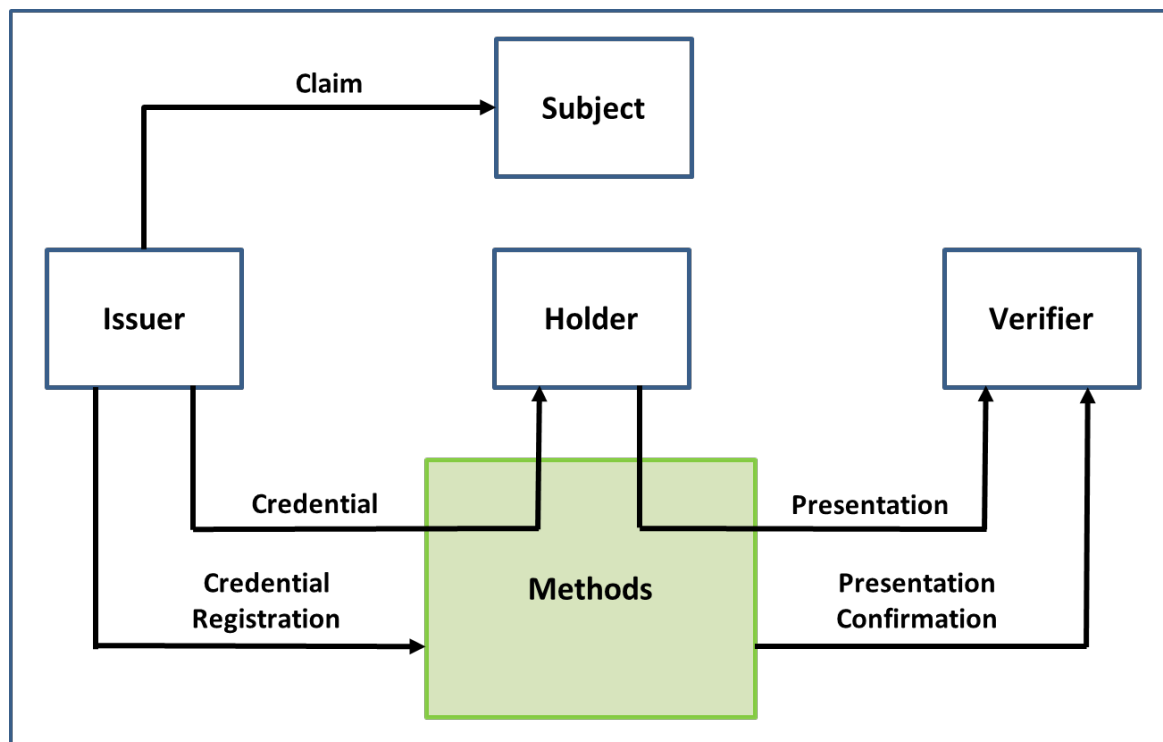


Figure 10: Digital Ecosystem Roles and Information Flows

8.1 Roles

8.1.1 The model shall consist 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; for example, when a parent (the Holder) controls the birth certificate (the Credential) of their child (the Subject).
4. **Verifier:** An Entity that accepts a Presentation from a Holder for the purposes of delivering services or administering programs.

- 8.1.2 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, Delegated Service Provider, Producer
Subject	Person, Organization
Holder	Digital Credential Holder, Card Holder
Verifier	Relying Party, Credential Service Provider, Identity Service Consumer, Delegated Service Provider, Consumer

NOTE 1: 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).

NOTE 2: In addition to the four roles outlined above, digital ecosystem actors include Supporting Infrastructure providers such as Network Operators.

8.2 Information Flows

- 8.2.1 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. An example of a Credential having more than one Subject is a marriage certificate.
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 of the Presentation. 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.

9 Atomic processes in detail

9.1 Identity Domain Processes

Identity Information Determination

Process Description	Identity Information Determination is the process of determining the identity context, the identity information requirements, and the identifier.
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

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 population through the use of identity information.
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

Identity Establishment

Process Description	Identity Establishment is the process of creating a record of identity of a Subject within a population.
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.
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 foundational event (e.g., birth, death, bankruptcy)
Output State	Continuous Presence: The identity exists continuously over time in association with many transactions

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

9.2 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 within a 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 are 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 foundational 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

9.3 Credential Domain Processes

Credential Issuance

Process Description	Credential Issuance is the process of creating a Credential from a set of Claims about one or more Subjects 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 verification attempts, 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. 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

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

9.4 Consent Domain Processes

Consent Notice Formulation

Process Description	Consent Notice Formulation is the process of producing a consent notice statement that describes what <i>personal information</i> is being, or may be, collected; to which parties the <i>personal information</i> is being disclosed (as known at the time of presentation); for what purposes the <i>personal information</i> is being collected, used, or disclosed; the risk of harm and other consequences as a result of the collection, use, or disclosure; how the <i>personal information</i> will be handled and protected; the time period for which the consent notice statement is applicable; under whose jurisdiction or authority the consent notice statement is issued; and the rights of and process to revoke any consent given in whole or in part pursuant to such consent notice. 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, the identity information of 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 or revocation 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

9.5 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 a signature is valid.
Input State	Signature: A signature exists
Output State	Checked Signature: A signature is valid

10 Qualifiers in detail

10.1 Identity Domain Qualifiers

10.1.1 The PCTF recognizes identity domain qualifiers that are based on the two identity types:

- **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, driver licensing, or social media). Depending on the identity context, a contextual identity may be tied to a foundational identity (e.g., a driver's 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.

10.2 Pan-Canadian Levels of Assurance (LOA) Qualifiers

Pan-Canadian Identity Assurance Levels (Persons)	
Qualifier Value	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 Value	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 Value	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 Value	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.

10.3 Signature Domain Qualifiers

- 10.3.1 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”.
- 10.3.2 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.

10.4 Other Trust Framework Qualifiers

- 10.4.1 Qualifiers may be based on the three levels of assurance defined by the *European Regulation No 910/2014* on electronic identification, authentication, and trust services (eIDAS) for electronic transactions:
- **Low:** Low degree of confidence.
 - **Substantial:** Substantial degree of confidence.
 - **High:** High degree of confidence.
- 10.4.2 Qualifiers may be based on the 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.

Annex A: Identity Management Overview

(Informative)

This annex provides a general overview of specific topics in identity management.

A.1 Identity

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

An identity must be unique. 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.

A.2 Defining the Population

Those Entities that fall within the mandate of a program or service constitute the population of interest of the program or service.

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

A.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.

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/service context

A.4 Determining Identity Information Requirements

A property or characteristic associated with an identifiable Entity is referred to as an identity attribute. Examples of identity attributes for a person include *full 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 sufficient to distinguish one Entity from all other Entities within the program/service population (i.e., achieve the uniqueness requirement for identity).

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/service eligibility). Note that the use of organizational information is not constrained by privacy legislation.

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. 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 the identity information and program-specific personal information occurs, it is a good practice to describe both purposes. This ensures that the use of the 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 the identity information and program-specific personal information as much as possible.

A.4.1 Identifier

The set of identity attributes that is used to uniquely distinguish a particular Entity within a population is referred to as an *identifier*. This set of identity attributes constitutes 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/service may specify *full name* and *date of birth* as the identifier set of identity attributes. Another program/service may specify *full name*, *date of birth*, and *place of birth* as the identifier set of identity attributes. Yet another program/service may use an assigned identifier (such as a health insurance number or a business number) as the identifier set of identity attributes.

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

- **Universality** – Every Entity within the population of interest must possess the identifier set of identity attributes. However, even when an identity attribute is universal, widespread missing or incomplete values for the identity attribute may render it useless as part of an identifier set. For example, many dates of birth for persons born outside of Canada consist only of the year or the year and the month.
- **Uniqueness** – The values associated with the identity attributes must be sufficiently different for each Entity within the population of interest so that the Entities within the population of interest 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 in cases where the full name of a person would suffice).

A.4.2 Assigned Identifier

It is generally agreed that *full name* and *date of birth* comprise the minimum set of identity attributes required to constitute an identifier for a person. Analyses¹ have shown that a combination of *full name* (i.e., *last name* + *first given name*) and a complete *date of birth* will distinguish upwards of 96% of the persons in any population. While adding other identity attributes (e.g., *place of birth*) to the set of identity attributes 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.

However, before an assigned identifier can be associated with an Entity, the uniqueness of the Entity's identity within the population of interest must first be established (i.e., Identity Resolution must be achieved) through the use of other identity attributes (e.g., *full 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/service that maintains them.

¹ NASPO IDPV Project, Report of the IDPV Identity Resolution Project, February 17, 2014

- Assigned identifiers maintained by one program/service may be provided to other programs/services so that those programs/services can also use the assigned identifier to distinguish between different Entities within their populations of interest; 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.

A.5 Identity Resolution

Identity Resolution is defined as the establishment of the uniqueness of an Entity within a 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 of interest. Since the identifier is the set of identity attributes that is used to uniquely distinguish a unique and particular Entity within a population, the identifier is the means by which Identity Resolution is achieved.

A.6 Ensuring the Accuracy of Identity Information

Identity information must be accurate, complete, and up to date. 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 may change over time as a result of the occurrence of a foundational event (e.g., death of a person, dissolution of a corporation). 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.

Annex B: Legal Entities

(Informative)

B.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.

B.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.

Annex C: Relationships in Detail

(Informative)

C.1 Relationship Models

C.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).

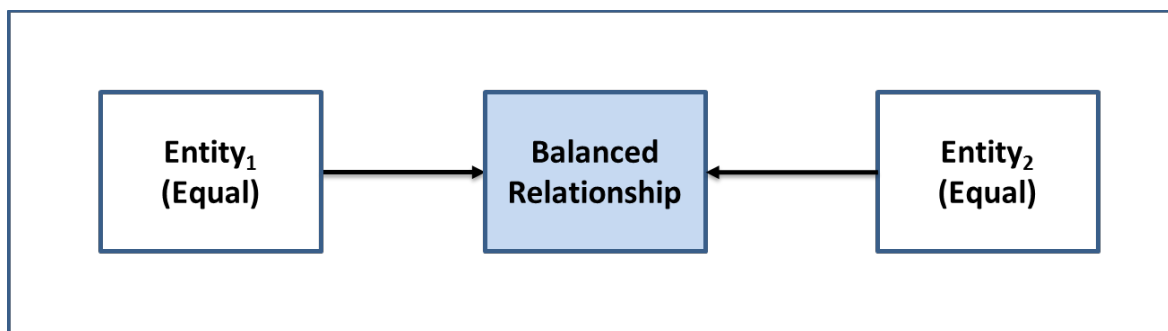


Figure 3: The Balanced Relationship Model

C.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).

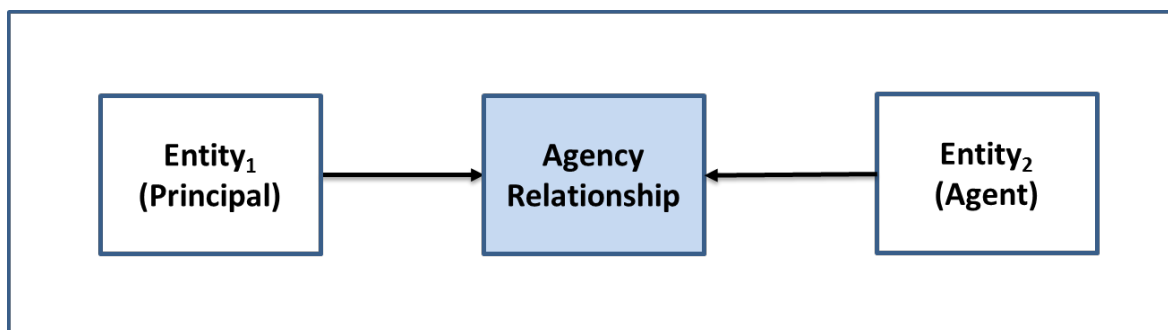


Figure 4: The Agency Relationship Model

The Relationship between the Principal and the Agent is a contractual one. Therefore, the rights and duties of the Principal and the Agent 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 means by which a Principal appoints another Entity as an Agent and confers upon the Agent the authority to perform certain acts on behalf of the Principal can be through any type of contract or agreement. Hiring a real estate agent, a lawyer, or an accountant are all forms of agency establishment.

C.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).

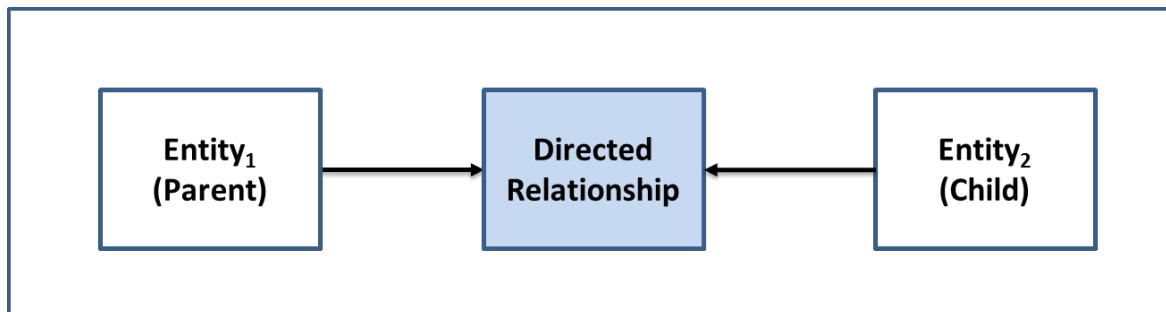


Figure 5: The Directed Relationship Model

C.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 Relationship or a Directed Relationship. This is illustrated in Figure 14.

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.

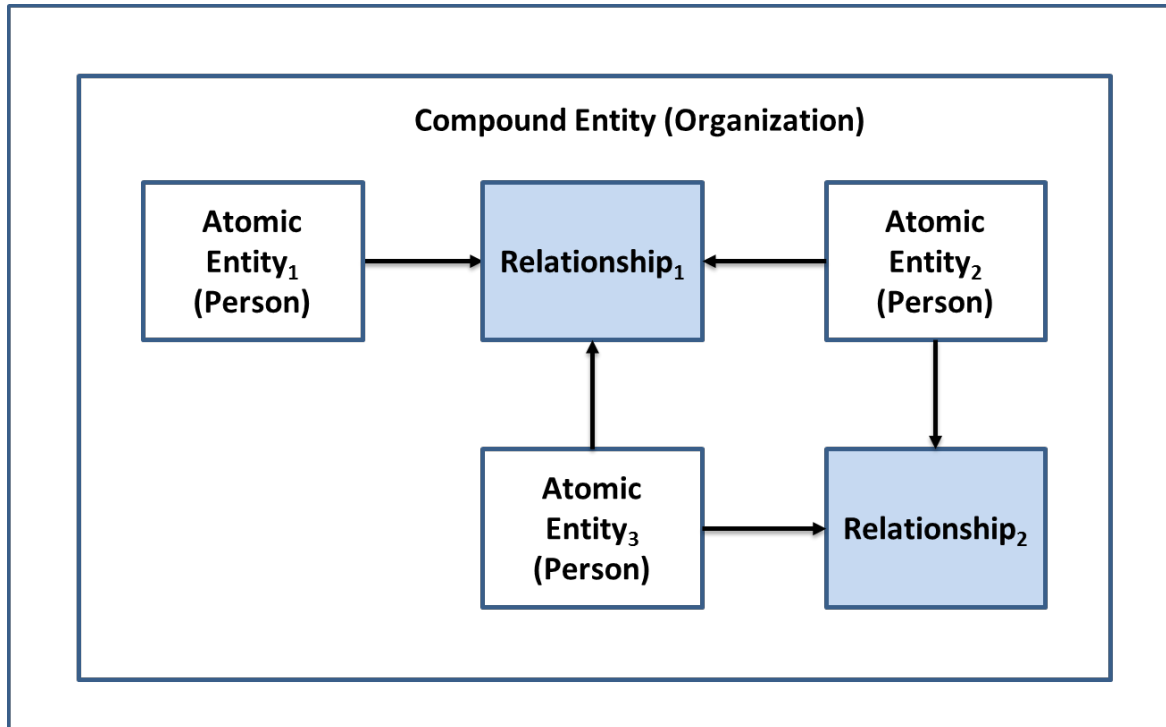


Figure 6: An Internal Relationship Network within an Organization

C.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.

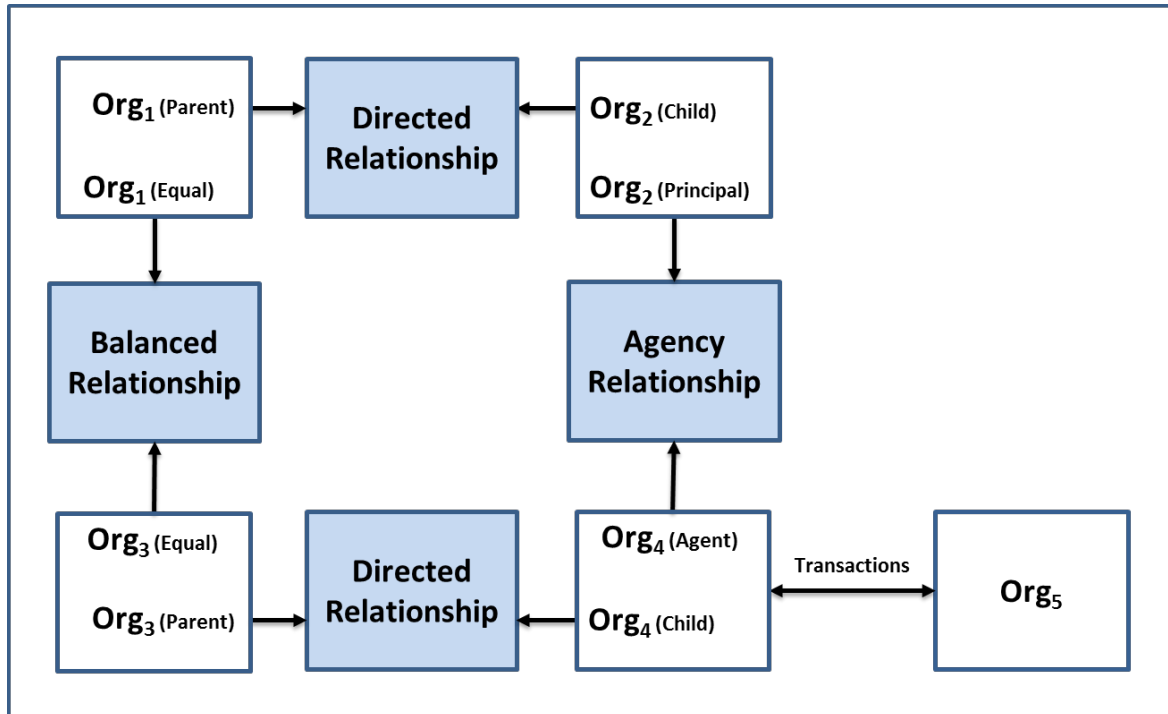


Figure 7: Organization to Organization Relationships

NOTE: Relationships between Entities must be differentiated from *interactions* between Entities (i.e., transaction execution). In Figure 15 above, **Org₄** has interactions with **Org₅**, but **Org₄** does not have a Relationship with **Org₅**. This concept will be discussed in more detail at a future date.

Annex D: Credentials Overview

(Informative)

D.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 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). Stated more precisely, a Credential contains a set of one or more Claims asserted about one or more Subjects. 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 to issue the Credential. The Holder can present the Credential to a Verifier in order to meet the program or service requirements of the Verifier.

D.2 Types of Credentials

The following is a list of some of the many types of Credentials that exist, along with some examples of their documentation:

- 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)
- Health Credentials (e.g., “vaccine passport”, vaccination certificate)

- 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)
- System Access Credentials² (e.g., user name/password combination)

D.3 Information Contained in a Credential

The PCTF Credential Model, defines the three types of information that are contained within a Credential: the Credential Metadata, the Credential Payload, and the Credential Proofs.

D.3.1 Credential Metadata

The Credential Metadata consists of information about the Credential itself. This information is expressed by means of a set of Credential Attributes. Some examples of Credential Metadata are:

- Information that uniquely identifies the instance of the Credential (e.g., a document identifier, a passport number, a birth certificate number, a banking credential identifier)
- 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).

² Information systems commonly use System Access 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 a System Access Credential. Some information systems use other forms of authenticators, such as biological characteristics (e.g., facial photo, fingerprints, voice, retinas) or public key certificates.

D.3.2 Credential Payload

The second type of information contained within a Credential consists of a set of Claims that are asserted about the Entities who are the Subjects of the Credential. This set of Claims is known as the Credential Payload. These Claims are expressed by means of Entity Attributes that describe the properties or characteristics of the Entities who are the Subjects of the Credential. These Entity Attributes can be a combination of identity attributes of the Subjects and non-identity attributes of the Subjects. Some examples of identity attributes of a Subject are: the Subject's full name and the Subject's date of birth. 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 assets³.

If a Credential asserts that there is a Relationship between the Subjects, then the Credential Payload will also include Relationship Attributes.

It should be noted that there exists the concept of an *anonymous Credential* (a.k.a. a *pseudonymous Credential*). An anonymous Credential is a Credential that, while still making an assertion about an Entity, does not reveal the Entity's identity. Anonymous Credentials provide Entities with a means to prove statements about themselves (e.g., I am 18 years of age or older; I am in control of this Credential (i.e., I am the Holder of this Credential)) and their relationships with other Entities (e.g., I am married; I am a parent) while maintaining their anonymity. An anonymous Credential may contain a Subject's identity attributes (such as an assigned identifier) but still be treated as an anonymous Credential if the identity attributes are not intended to be used for Identity Resolution purposes.

D.3.3 Credential Proofs

The third type of information contained within a Credential is what is referred to as Credential Proofs. Credential Proofs are one or more methods or mechanisms that are used to verify that the Issuer authored the Credential, that the Credential has not been tampered with, and that the Credential has been bound to a Holder.

Over the years a variety of methods have been employed to verify a Credential's authorship as well as providing evidence of Credential tampering: a wax seal on a document, a security hologram on a passport, an encrypted information chip on a credit card, a digital signature, a Verifiable Credential.

³ In addition, the Credential Attributes of the Credential (in particular the *Credential Type* Attribute) may provide non-identity information about the Subjects (e.g., 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, the Subjects are married).

A Credential is bound to a Holder by means of the Credential Authenticator Binding process (i.e., the process of associating a Credential issued to a Holder with one or more authenticators). Subsequently, the Credential Verification process uses the authenticators bound to an issued Credential to verify that a Holder has control over an issued Credential. The authenticators bound to an issued Credential are used to prove that the Credential is referring to the same Holder that was originally bound to the Credential.

D.4 Documentation of a Credential

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 a digital form (i.e., Digital Credentials). The documentary evidence of a Credential can be thought of as a *container* or as a substrate for transporting the Credential. In the PCTF Credential Model, the Credential is placed inside the container and becomes the *payload of the container*.

D.5 The PCTF Credential Model

Figure 16 illustrates the PCTF Credential Model.

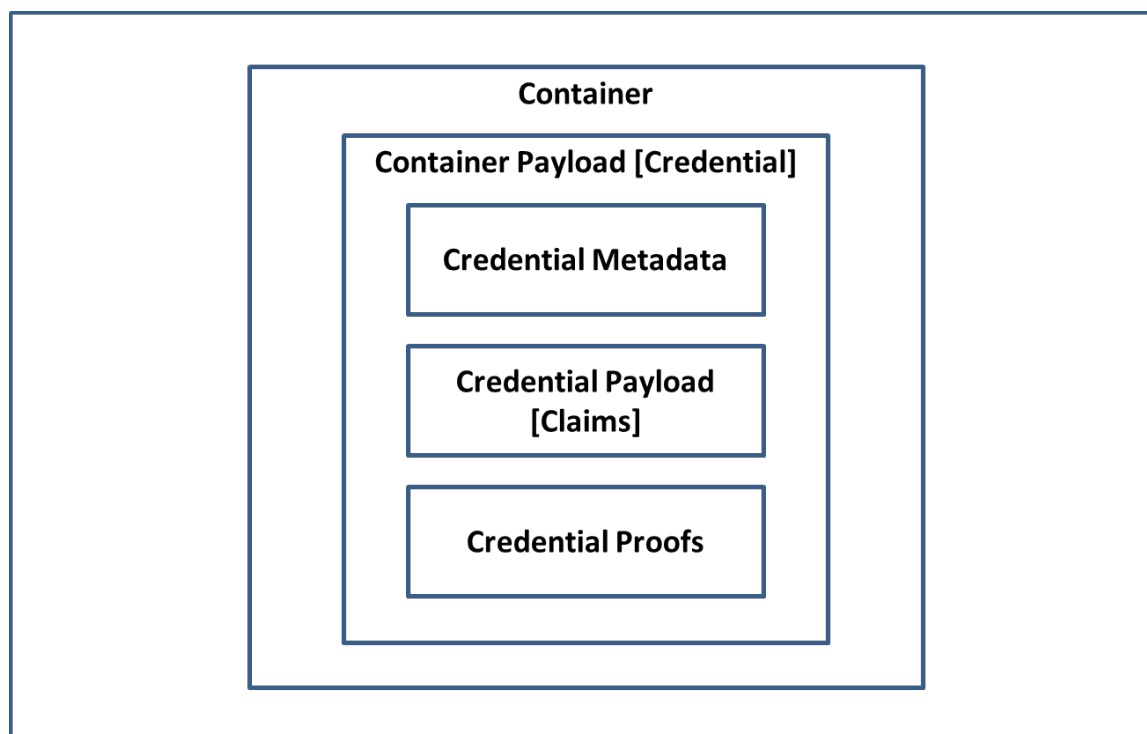


Figure 8: The PCTF Credential Model

As described previously, 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, that the Credential has not been tampered with, and that the Credential has been bound to a Holder.

NOTE: 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 stating that the Verifier has confidence that the Issuer of the Credential has properly ascertained the veracity of the Claims prior to creating the Credential Payload.

D.6 PCTF Claims Assertion Models

D.6.1 The PCTF 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 PCTF Claims Assertion Model of a Subject Claim.

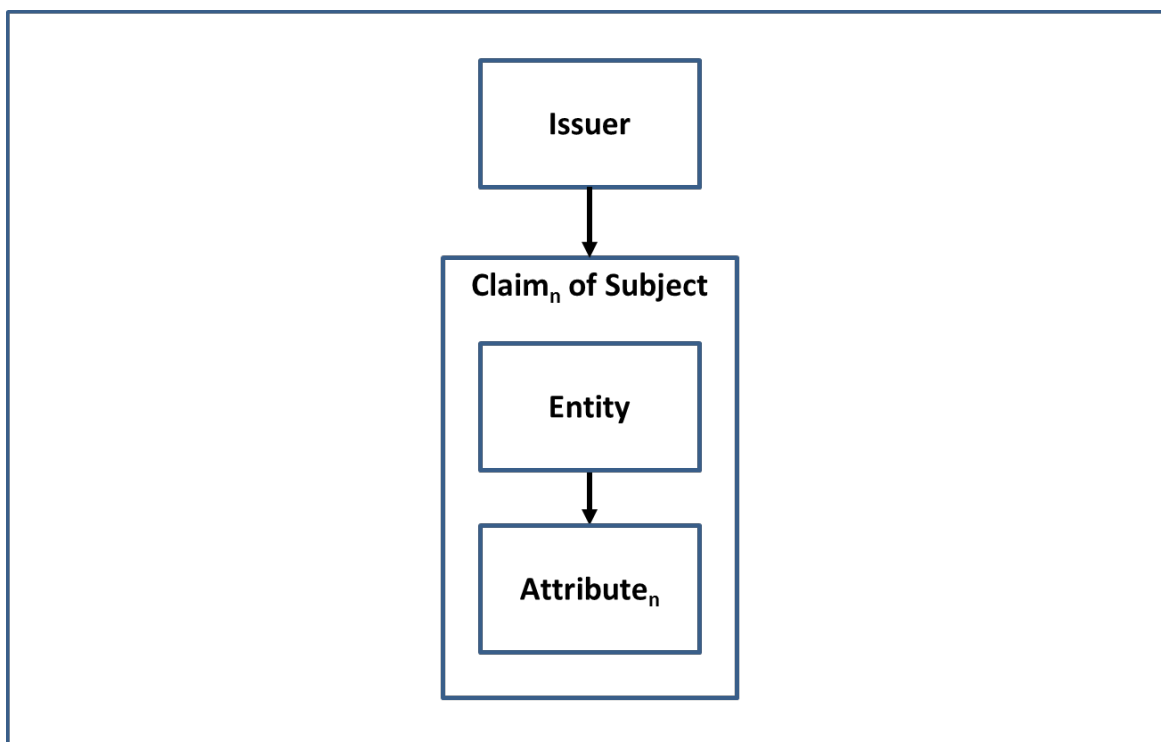


Figure 9: The PCTF Claims Assertion Model of a Subject Claim

D.6.2 The PCTF 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 PCTF Claims Assertion Model of a Relationship Claim.

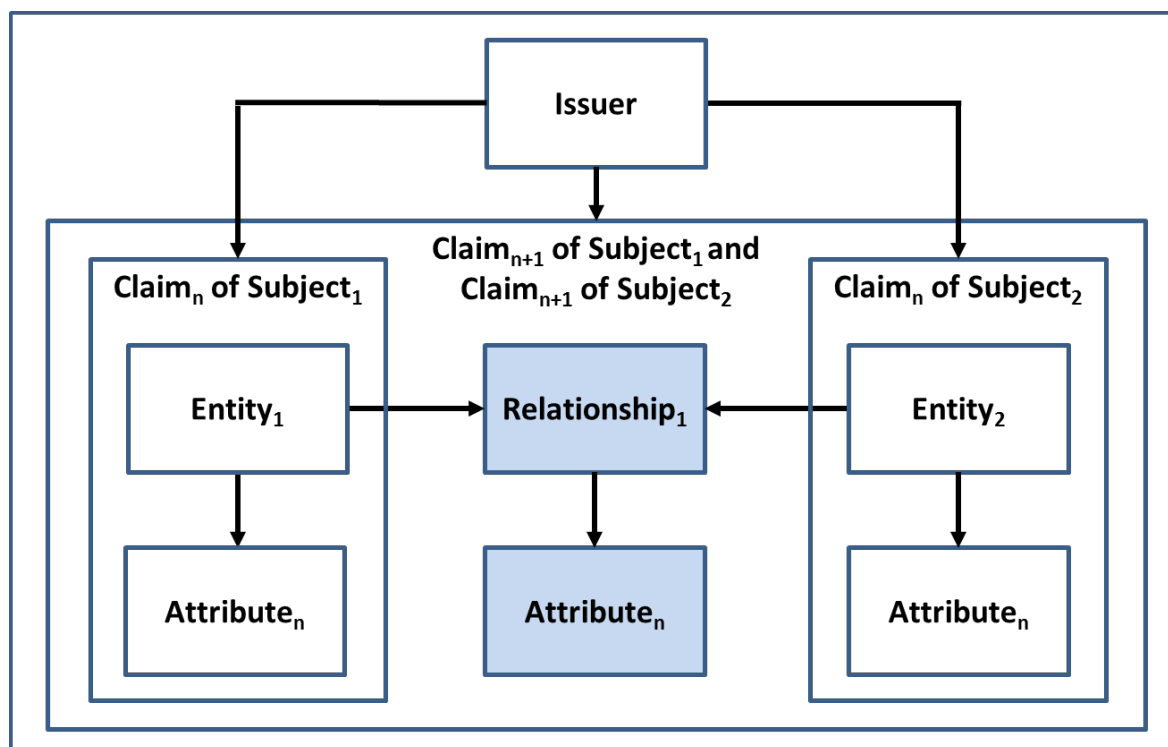


Figure 10: The PCTF Claims Assertion Model of a Relationship Claim

D.7 The PCTF Credential Issuance Model

In the PCTF 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 PCTF Credential Issuance Model.

NOTE: Some implementations of a Credential Issuance process may include other steps and outputs. The definition above is the minimum necessary for conformance with the PCTF specification, but not necessarily sufficient to meet the documented goals of a credential management system.

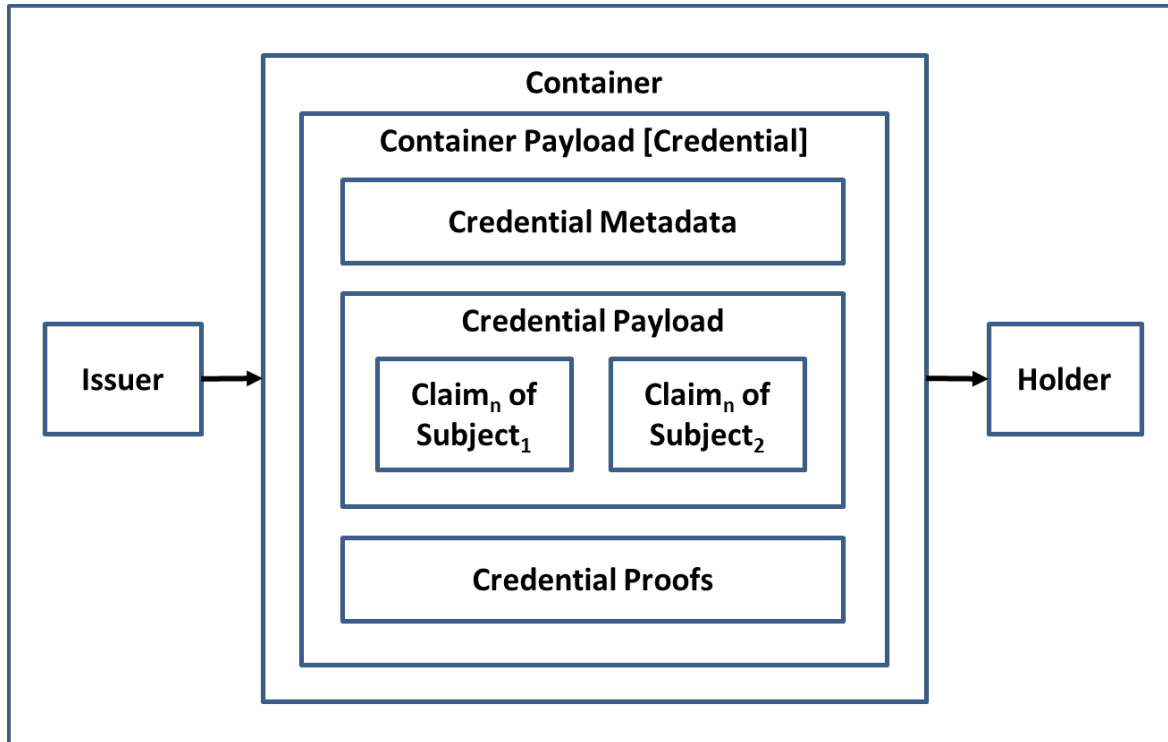


Figure 11: The PCTF Credential Issuance Model

Annex E: Identity Verification in Detail

(Informative)

Identity Verification is the process of confirming that the identity information is under the control of the Subject. Identity Verification can only be applied to Atomic Entities (i.e., persons). It should be noted that the Identity Verification process may use personal information that is not part of the Subject's identity. There are four recognized methods used to achieve Identity Verification:

Knowledge-based confirmation: An Identity Verification method that uses personal information or shared secrets to prove that the Subject presenting the identity information is in control of the identity. Knowledge-based confirmation is achieved by means of the challenge-response model: the Subject 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 Subject 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 Subject presenting the identity information.

Physical possession confirmation: An Identity Verification method that requires physical possession or presentation of evidence (e.g., a Credential) to prove that the Subject 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 Subject 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.

Annex F: Credential Verification in Detail

(Informative)

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.

NOTE: The degree of control over the issued Credential can be used to generate a level of assurance.

F.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 owns and controls (e.g., a cryptographic hardware key, a phone, a computer, etc.). Caution must be exercised because someone can impersonate the Holder by taking control of their device. The fraudulent re-registration of a Subscriber Identity Module (SIM) or “SIM Swap” is an example of how a device can be stolen “virtually” from the proper Holder. Ownership authentication should be used in conjunction with one of the other authentication methods, ideally biometric authentication.
- Something the Holder knows (e.g., a password, a response to a challenge question, a one-time-password). The exclusive use of secrets such as passwords should be treated with extreme caution since passwords can be stolen by means of a wide array of methods and as a result, passwords can be changed without the Holder’s or Issuer’s knowledge or involvement. As a rule, knowledge-based authentication should only be used in conjunction with one of the other authentication methods.
- Something the Holder is or does, i.e., the Holder’s biometrics (e.g., face, fingerprints, retinas, keyboard stroke timing, gait). The use of a biometric authenticator should incorporate liveness and similar presentation attack defenses to prevent spoofing of the biometric. Biometric authentication should be used in conjunction with one of the other authentication methods, ideally ownership authentication. This is because biometric authentication should require the active knowledge and/or involvement of the Holder and is therefore dependent on the Holder’s active control of the device which processes the biometrics.

It should be noted that the irrevocability of biological characteristics (e.g., face, fingerprints, retinas) makes the use of biometric authentication attractive for Credential Verification. A Holder’s biological characteristic cannot be easily changed. Nor can a Holder’s biological characteristic be easily replicated; nonetheless, industry standards include requirements for robust liveness detection and similar anti-spoofing techniques to protect against biometric replication attempts.

However, industry standards are generally cautious in regards to the exclusive use of biological characteristics as authenticators for Credentials. Biometric authentication should be used in conjunction with ownership authentication.

Annex G: Guidelines on Mutual Recognition

(Informative)

This annex outlines some general guidelines on mutual recognition.

G.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 which will be responsible for the assessment 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/service.
- **Site Visit.** If possible, 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/service 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 the 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.

G.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/service or business line. The scope of the mapping may include upstream programs/services 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/services under assessment will be well-established and will be using terminology developed 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 program, may be the same as or be different from a subsequent “enrolment” in a service that has accepted a Digital Credential. The mapping of the atomic processes can help to clarify what may be a duplicate (i.e., redundant) process, and what may be specifically required for the service.

G.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 to date 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 criterion has been met;
- **Accepted with Observation** – The conformance criterion has been met, but a dependency or contingency over which the assessed party might not have direct control has been noted;

- **Accepted with Recommendation** – The conformance criterion has been met, but a potential improvement or enhancement should be implemented in the future;
- **Accepted with Condition** – The conformance criterion has not been met, but the process is accepted due to the demonstration of safeguards, compensating factors, or other assurances in place;
- **Not Accepted** – The conformance criterion has not been met; or
- **Not Applicable** – The conformance criterion does not apply.

G.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 Credential;
- Be signed by the person/organization/jurisdiction accepting the Digital Credential at a given qualifier level;
- Include the specific scope or use of the Digital Credential, 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.

Annex H: Thematic Issues

(Informative)

The CAN/CIOSC 103-0 Working Group has identified several high-level thematic issues that should be addressed in order to advance the digital ecosystem.

Thematic Issue 1: Foundational Identity (Priority: High)

A revised definition of foundational identity is needed. The current definition is more concerned with what *triggers* the creation or modification of a foundational identity – it does not clearly define what a foundational identity is.

Status: In Progress.

Thematic Issue 2: Interactions between Entities (Priority: High)

Relationships between entities must be differentiated from interactions between entities (i.e., transaction execution). A new section is required that explains this concept.

Status: In Progress.

Thematic Issue 3: Unregistered Organizations (Priority: High)

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

Status: In Progress.

Thematic Issue 4: Informed Consent (Priority: Medium)

The current version of this 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.

Status: Not Started.

Thematic Issue 5: Privacy Concerns (Priority: Medium)

In regard 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 PCTF is required to determine if these atomic processes are appropriate.

Status: Not Started.

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

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). It remains to be determined how such multi-actor assessments will be conducted.

Status: Not Started.

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

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

Status: Not Started.

Thematic Issue 8: Signature (Priority: Low)

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

Status: Not Started.

Bibliography

- [1] Canadian Joint Councils. Canadian Joint Councils' Digital Identity Priority: Public Policy Recommendations. 2018
- [2] CAN/DGSI 103-1:2023, Digital Trust and Identity – Part 1: Fundamentals
- [3] CAN/DGSI 103-3:2024, Digital Trust and Identity – Part 3: Digital credential management system
- [4] Communications Security Establishment. ITSP.30.031 User Authentication Guidance for Information Technology Systems
- [5] European Union. Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market
- [6] GPG 43, Requirements for Secure Delivery of Online Public Services
- [7] GPG 44, Authentication Credentials in Support of HMG Online Services
- [8] GPG 45, Identity Proofing and Verification of an Individual
- [9] GPG 53, Transaction Monitoring for HMG Online Service Providers
- [10] ICAO MRTD Doc 9303 series of standards, Machine Readable Travel Documents
- [11] ISO 18013-5, Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application
- [12] ISO/IEC 24760-1:2019, IT Security and Privacy -- A framework for identity management -- Part 1: Terminology and concepts
- [13] ISO/IEC 24760-2:2015, Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements

- [14] ISO/IEC 24760-3:2016, Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice
- [15] ISO/IEC 27018, Information Technology – Security Techniques – Code of Practice for Protection of PII in Public Clouds Acting as PII Processors
- [16] ISO/IEC 29100, Information Technology – Security Techniques – Privacy Framework
- [17] ISO/IEC 29115:2013, Information technology -- Security techniques -- Entity authentication assurance framework
- [18] NIST Special Publication 800-63 Series, Digital Identity Guidelines
- [19] Office of the Privacy Commissioner of Canada. Guidelines for Obtaining Meaningful Consent. 2018
- [20] Treasury Board Secretariat of Canada. Directive on Identity Management. 2019
- [21] Treasury Board Secretariat of Canada. Federating Identity Management in the Government of Canada. 2011
- [22] Treasury Board Secretariat of Canada. Guideline on Defining Authentication Requirements. 2012
- [23] Treasury Board Secretariat of Canada. Guideline on Identity Assurance. 2017
- [24] Treasury Board Secretariat of Canada. Pan-Canadian Assurance Model. 2010
- [25] Treasury Board Secretariat of Canada. Pan-Canadian Approach to Trusting Identities. 2011
- [26] Treasury Board Secretariat of Canada. Standard on Identity and Credential Assurance. 2013
- [27] W3C. Verifiable Credentials Data Model 1.0
- [28] W3C. Verifiable Credentials Implementation Guidelines 1.0

[29] W3C. Verifiable Credentials Use Cases