Pan-Canadian Trust Framework Model Draft Recommendation V1.0

This Draft Recommendation has been developed by the Digital ID & Authentication Council of Canada (DIACC) Trust Framework Expert Committee (TFEC). The TFEC operates under the controlling policies of the DIACC. Comments submitted by the public are subject to the DIACC Contributor Agreement.

DIACC expects to modify and improve this Draft Recommendation based upon public comments. The purpose of the open commentary is to ensure transparency in development and diversity of truly Pan-Canadian input. Comments made during the review will be considered for incorporation to the next draft. DIACC will prepare a disposition of comments to provide transparency with regard to how each comment was handled.

Forthcoming PCTF releases will expand, clarify, and refine the content of this document. The intended target audience is inclusive of decision makers who may or may not be domain technology experts.

When reviewing this draft recommendation, please consider the following:

1. Do you agree with "Digital Representation" to refer to the information of concern? Agree or suggest a new term.
2. Does the document strike an appropriate balance between being forward-looking and considering the current status quo?
3. Does the document contain a sufficient level fo detail for a broad overview, bearing in mind PCTF components and profiles will address many details considered out of scope for this document?
4. Do the trusted processes and associated descriptions cover all of the major processes with which the PCTF should be concerned?

Table of Contents

1. Introduction

As service delivery becomes increasingly digital, individuals, governments, and businesses realize a need to trust information about those with whom they interact; that the person at the other end of a connection is who he or she purports to be, or that information about that person is correct. Service providers and their clients also need to know that this information is protected as it travels across networks and organizational boundaries, and as it is captured in legal documents as evidence of a transaction. This is particularly true in high-value or high-sensitivity transactions that are currently difficult to conduct digitally. Such transactions include certain financial transactions, purchasing real estate, submitting a response to a request for proposals, accessing health records, purchasing controlled goods online, or managing government benefits on behalf of an elderly parent.

In response, governments and industries around the world are developing frameworks to promote trusted environments online. Such frameworks typically consist of a set of auditable business and technical requirements for processes. Legal requirements may also be referenced in the framework. Commonly known as trust frameworks, these frameworks enable secure and private interactions between parties and across various networks and organizations. Many existing financial, supply chain management, and digital identity networks are based on some form of trust framework. Trust frameworks are a more scalable, more transparent, and arguably more economical approach to creating a trusted environment than a diverse assortment of private agreements between few organizations. They have the added benefit of providing enhancements and catalysts that can accelerate the pace of and increase the adoption rate of shared systems when compared to other approaches.

The Pan-Canadian Trust Framework (PCTF) is a trust framework for trusted digital representations (i.e., identities, attributes, relationships) of people and other types of entities in Canada.

Since the PCTF is intended for use by a range of stakeholders in different communities, any stakeholder can adopt the requirements of the PCTF. In so doing, that stakeholder demonstrates a willingness to adhere to accepted conventions, which results in increased levels of trust and assurance among the stakeholder's clients, business partners, etc.

1.1 About this Document

The purpose of this document is to provide a high-level model overview of the PCTF. It includes a recap of contextual information and PCTF goals and objectives.

This document also outlines functional areas that are the primary focus of the PCTF. The outline (provided in Section 5) provides a general sense of the digital representations with which the PCTF is concerned and the various processes involved in creating, managing, and using these digital objects.

Individual PCTF components and profiles provide detailed descriptions of the processes highlighted in this document.

The audience for this document includes:

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

2. About the PCTF

2.1 Context

Technology and services that allow people to interact with governments, businesses, and each other with digital convenience and efficiency offer considerable potential for social and economic innovation and development. The ability to trust information about participants in these interactions is an essential pre-requisite to realizing this potential. The PCTF supports this aspect of digital services as a trust framework providing consistent and auditable processes for the creation, management, and use of digital representations of people and other entities.

However, to be successful, the use of digital representations must scale beyond a limited number of relationships. It must scale beyond limited one-off integrations. With clients, customers, and users a prime focus for most stakeholders, digital representations of these entities must be accepted between service providers, economic sectors, levels of government, and jurisdictions. In practice, this means individuals and other participants must be able to use and manage information about themselves in multiple contexts across the economy.

A high degree of interoperability requires mutual trust. Service providers need to know who they interact with digitally. Service consumers, individuals or otherwise, need to trust the identity of the services with which they interact. Without interoperability and trust, Canada risks continued existence of organizational, policy, and technical barriers that have:

- contributed to an excess of verification procedures, registrations, accounts, passwords, usernames, user profiles, and the systems needed to administer them all; and
- hampered modernization efforts that foster innovation and improve service experience, efficiency, and effectiveness.

Moreover, Canadians expect their digital identity ecosystem to operate with transparency, ensuring fairness for all and promoting privacy rights by design. They expect clear and meaningful notice about why and how information about themselves is collected, managed, and disclosed.

2.2 Goal

The goal of the PCTF is to enable and support the establishment of an innovative, secure, and privacy-enhancing Canadian digital identity ecosystem—which also respects fundamental human rights in the digital era—across the economy. In this respect, the PCTF seeks to facilitate the migration of traditional or complex face-to-face interactions to digital interactions that put people at the centre of the digital identity ecosystem while recognizing analogue business processes will continue to exist for some time.

To support development of a Canadian digital identity ecosystem, the PCTF adopts a pan-Canadian approach to digital identity, founded on broad-based agreement on principles and standards to develop solutions for use by all Canadians.

The PCTF supports development of a Canadian identity ecosystem by:

- ensuring the Canadian digital identity ecosystem is trustworthy – by putting control in the hands of consumers while encouraging a fair, innovative, and competitive environment for participants;
- focussing on transparency and privacy regarding usage and disclosure of personal information;
- supporting inclusion of participants offering a broad range of services;
- identifying applicable existing policy and technology standards that for the ecosystem; and
- maintaining a forward-looking perspective and revealing future areas for collaboration, development, and standardization.

2.3 Objectives

The PCTF recognizes that while there are dependencies and differences between jurisdictions, industries, and individual participants, a uniform approach to ecosystem development can be achieved by consistently implementing broadly accepted standards. Accordingly, objectives of the PCTF focus on ensuring the trustworthiness of the Canadian digital identity ecosystem by:

1. Defining participant roles and functions within the ecosystem. This document describes these roles, functions and associated processes in broad terms as a model for the PCTF. PCTF components and profiles provide more detailed requirements and guidelines as required.
2. Facilitating interactions within the ecosystem by defining requirements and guidelines that establish a level of trustworthiness for processes performed by ecosystem participants. PCTF components provide detailed descriptions and technical specifications of these requirements.

2.4 Scope

Success of the Canadian digital identity ecosystem will be dependent on users; users must trust the system and at all times be in control of it. The PCTF establishes a trust framework within which innovative solutions can be developed, measured and recognized. It defines conformance criteria necessary for digital identity ecosystem participants to interact with assurance.

As with other trust frameworks, the PCTF does not define a system or product per se. Similarly, the PCTF does not address commercial aspects of the ecosystem, such as commercial models, pricing, liability, intellectual property rights, and insurance.

2.5 Guiding Principles

The PCTF achieves its goals and objectives in part through standards and guidelines that reflect the following guiding principles:

1. **Support robust, secure, scalable solutions** – Canada's digital identity ecosystem must be sufficiently robust to ensure security, availability, and accessibility at all times.
2. **Implement, protect, and enhance privacy by design** – Privacy enhancing tools enable an individual to manage their information and what specified purpose(s) it is used for. These tools may include support for a user's "right to be forgotten" (when appropriate in the legislative context of the trust framework participant).
3. **Be inclusive, open, and meet broad stakeholder needs** – Digital identity ecosystem services and tools must be affordable, standardized, and create value for users in the interest of broad adoption and benefit to all Canadians.
4. **Be transparent in governance and operation –** Canadians need to trust that services offered in the Canadian digital identity ecosystem will respect and meet their needs and expectations.
5. **Provide Canadians choice, control, and convenience** – Services are based on the principle that individuals can choose what information to share, what services to use and from which countries, and are informed about the potential benefits and consequences of digital identities.
6. **Build on open standards-based protocols –** Use of open standards and applicable best practices for Canada's digital identity ecosystem helps protect against obsolescence, ensure interoperability, and foster a dynamic and competitive solutions marketplace.
7. **Maintain international interoperability –** Interoperability and global technology and policy standardizations are foundational to todays connected world. Much like standardized railway gauges enable travel and the movement of goods across countries, technology and policy interoperability and standardization allows digital services to communicate and lower costs while increasing innovation opportunities.
8. **Be cost effective and open to competitive forces –** It is essential that the digital identity ecosystem respects the budgetary constraints of the present and the future. Ensuring the ecosystem is open to competition, representing multiple economic sectors, each playing different roles, will lead to decreased costs for all stakeholders and increased innovation.
9. **Support independent assessment, audit, and enforcement** – For Canadians to trust a digital identity ecosystem, governing controls must be put in place. On-going,

functionally independent, and third-party assessments provide one way to ensure that ecosystem stakeholders adhere to the trust framework requirements.

10. **Minimize data transfer between sources and avoid creation of new identity information repositories** – Users of digital identity ecosystem services should be asked to provide only the minimum amount of personal information needed in a given interaction.

3. Structure of the PCTF

The PCTF consists of the Model Overview (described in this document) and the following elements:

1. PCTF components
2. Conformance criteria
3. Trusted processes
4. PCTF profiles

Each of these items is described in this section.

3.1 PCTF Components

PCTF components define the trusted processes and conformance criteria for specific areas within the scope of the PCTF. The components refine, expand on, and provide additional detail not presented in this model overview.

The Notice and Consent component of the PCTF, for example, defines a set of processes used to formulate a statement and obtain a consent decision on that statement from a person authorized to do so. The requirements in the Privacy component of the PCTF ensure that systems follow privacy-respecting practices, ensuring personal information is properly collected, protected, maintained and, when requested, destroyed when part of the digital identity ecosystem.

The focus of the PCTF components is to specify common baseline of conformance criteria, trusted processes. Participants can extend and refine the baseline through PCTF profiles.

3.2 Conformance Criteria

Conformance criteria are applied as a standard or use existing standards and/or guidelines for the delivery of trusted processes in the public and private sectors. Conformance criteria are the requirements, specifications, recommendations, and guidelines, that comprise a standard for specific processes. Participants can use these criteria to inform design and development of their products and services.

The PCTF conformance criteria are intended to complement existing legislation and regulation; participants in the digital identity ecosystem are expected meet the applicable legislated requirements and regulations in their jurisdictions.

In keeping with the guiding principles for building on open standards and maintaining national and international interoperability, the PCTF accepts that:

- Existing standards and specifications may be incorporated into the PCTF conformance criteria by reference. This ensures broad compatibility and reduces duplication and overlap of content and technical specifications.
- Where existing standards are incorporated into the PCTF, primary consideration is given to a Canadian implementation. This may require that international standards be interpreted and applied in a Canadian context (e.g., with respect to Canadian privacy law or data sovereignty considerations). Existing standards may be incorporated into the baseline PCTF components or PCTF profiles.

PCTF conformance criteria are developed with the objective of ensuring compliance with the various criteria can be assessed to determine the trustworthiness of a given process.

3.3 Trusted Processes

A process is a business or technical activity (or set of such activities) that transforms an input condition to an output condition. A business or technical process that is designated as a trusted process is assessed according to conformance criteria defined in PCTF components and profiles. Figure 1 illustrates the trusted process model wherein a trusted process transforms an object's *input state* into an *output state*.

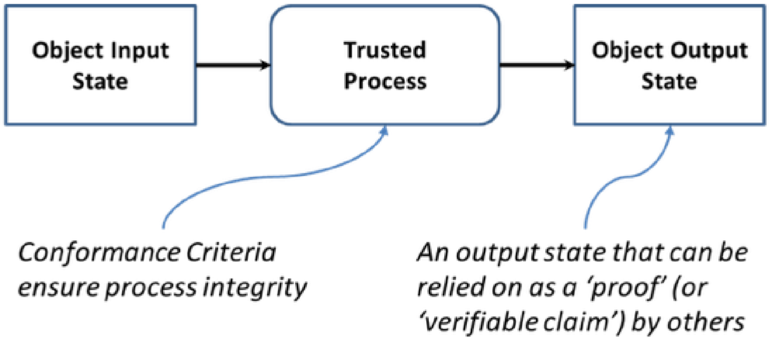
Object Input State
Trusted Process
Object Output State
Conformance Criteria ensure process integrity
An output state that can be relied on as a 'proof' (or 'verifiable claim') by others

Figure 1. Trusted Process Model

Trusted processes are crucial to ensuring the overall integrity of the digital identity ecosystem, and to the overall integrity of the Trust Framework. The integrity of a trusted process is paramount because the output of a trusted process is relied upon by many participants – across jurisdictional and sectoral boundaries, and, over the short-term and long-term. The PCTF ensures integrity of a trusted process through agreed upon and well-defined conformance criteria that enable a transparent and evidence-based assessment methodology. This explicit assessment is in contrast to many existing analogue processes that are trusted only to the extent that they enjoy wide adoption over a long timeframe.

An existing business or technical process may be designated as a trusted process that is subject to the conformance criteria, assessment process, and certification defined by the PCTF. For example, existing programs or services usually have embedded identity-related processes, sometimes referred to as identity-proofing or identity registration. Processes that were originally developed to work within a particular context (e.g., enrolling a person into a service, issuing a driver's license) may be leveraged and relied on as trusted processes within the PCTF. This is done by mapping the existing processes (or sub-processes) into the trusted process definitions. Once mapped, these processes can be assessed and certified using the defined conformance criteria associated with the corresponding trusted processes.

3.4 PCTF Profiles

The scope of the PCTF is very broad, seeking to provide a baseline standard across the Canadian economy in both public and private sector contexts. PCTF profiles allow industries, economic sectors, and other communities with shared interests to define how the PCTF will apply in specific contexts, use cases or to meet particular business needs.

PCTF profiles allow participants to tailor baseline conformance criteria to specific requirements or applications. This could include, but is not limited to:

- requiring mandatory compliance with all conformance criteria;
- defining levels of assurance;
- defining acceptable evidentiary sources;
- specifying acceptable technologies; or
- extending certain conformance criteria (e.g., requiring additional audit and logging processes).

4. Key Concepts

The PCTF is based on a small number of key concepts. Foremost is the idea that trust is created and can be assessed at multiple points in a chain of processes that create and use digital representations of people and other entities.

The key concepts can be summarized as:

- Participants in the digital identity ecosystem create, use and/or manage **digital representations**;
- When processing digital representations, participants assume one or more **roles** in the ecosystem;
- Each role performs a number of functions that are made up of one or more **trusted processes;** and
- Compliance with specified **conformance criteria** that define trusted processes.

The following sections provide a description these concepts in the PCTF context.

4.1 Digital Representations

A digital representation is an electronic dataset that refers to any type of entity that can be subject to legislation, policy, or regulations within a context, and which may have certain rights, duties, and obligations. Digital representations are intended to be mapped to model real-world actors, such as persons and organizations that benefit from the implementation or use of the PCTF.

Digital representations can be created and managed for entities other than people. Digital representations can be created and managed for:

1. **Persons –** An individual, human being. Examples of persons include residents of a jurisdiction (country, province, etc.), the customers of a business, and private individuals.
2. **Organizations –** An entity whose existence is established by legal statute or convention. Examples of organizations include businesses (including sole proprietorships, partnerships, and corporations), government agencies, co-operatives, and registered charities.
3. **Machines –** Software and hardware (potentially acting as intelligent agents). Typically, machines that act on behalf of a person or an organization are not autonomous identities in their own right. As the PCTF evolves, future technology that results in the creation of machines that exhibit some level of autonomy may result in conformance criteria and trusted processes specific to these types of entities.

Development of conformance criteria and trusted processes most closely related to "persons" is the priority for PCTF components. Those related to "machines" are lower priority in PCTF development.

4.2 Participant Roles

Digital representations go through a lifecycle that begins with creation, proceeds to active use (during which the data may change, be added or removed, etc.), and then to archival and, in some cases, destruction. Trust is created during the execution of key processes throughout this lifecycle. The PCTF defines standards and guidelines for these processes.

The key processes of a digital identity ecosystem fall into three broad functions:

1. Create and manage digital representations
2. Use digital representations
3. Enable digital identity systems

Ecosystem participants perform these functions. Participants are individual persons public, commercial, or non-profit organizations, and (increasingly), machines. In the PCTF model, participants that perform key processes in the lifecycle of digital representations assume one or more roles that are defined as follows in the PCTF context.

Function	**Role**	**Description**
Create and manage digital representations	Identity providers	Participants that create and manage identities. Sometimes referred to as identity service providers or identity issuers. In some cases, the subject is the creator and manager of its own identity.

	Credential providers	Participants that create and manage credentials. Sometimes referred to as attribute providers.
	Authenticator providers	Participants that create and manage authenticators. Sometimes referred to as credential service providers. These are not the same as PCTF Credential Providers. See section 5.1.2 for details.
Use digital representations	Relying parties	Participants who rely on digital representations created and managed by other participants.
	Digital representation subjects	The entity that the digital representation is representing. Typically, the entity to whom the digital representation is issued. In many use cases, the subject of a digital representation will assume explicit functions and/or responsibilities. There may also be implicit functions performed by the subject in the context of the digital identity ecosystem. For example, functions associated with a “motivation to recover” a digital representation when problems or suspicious events are detected.
Enable digital identity systems	Infrastructure providers	Participants that provide the physical and electronic infrastructure needed to enable digital interactions.
	Assessors	Participants that assess another participant’s compliance with the PCTF.

Given the variety of technical, service, and business models that define the ecosystem, roles may be performed by multiple different participants in a given context, or one participant may perform several roles (e.g., be a relying party as well as a credential provider).

There is also the potential for the PCTF to lower barriers-to-entry to the identity ecosystem; meaning that some organizations can reuse technology put in place by the PCTF participants, yet, not fully integrate to the PCTF for their own reasons (e.g., being cost or delays of conformance assessment, which could present a burden on start-up companies).

Governance Roles

As a trust framework intended for broad adoption, the PCTF defines governance roles for certain ecosystem stakeholders. Participants acting in these roles are responsible for drafting, maintaining, and helping ensure consistent adoption of the various components of the PCTF. Governance roles may also be extended to include governance of the use and application of the PCTF in the digital ecosystem.

5. Functional Outline

This section outlines the identity-related functions and processes that are in scope for the PCTF.

5.1 Creating and Managing Digital Representations

Functions in this category involve proving or checking the identity or characteristics of a real entity (e.g., a person) and creating a digital representation for that entity. Once a digital representation is created, it is managed through processes that allow for the data to be updated, deleted, and re-verified as required – with the goal of ensuring that representation remains current and accurate.

Currently, the PCTF defines three types of digital representation:

1. **Identity** – Information that makes it possible to identify a unique entity (e.g., personal information), either on its own or with supporting related information. Examples for persons include names, dates of birth, birth registrations (in the future), or biometrics. Examples for machines could include the serial number, a trusted digital certificate, or network MAC address.
2. **Credential** – Information describing attributes or properties of an entity. This information may exist on its own (e.g., as a credential that contains no personal information, only a unique string identifier) or be related to personal information. Examples include education levels (e.g., a university degree in engineering), permission to operate a vehicle (e.g., a driver’s license), income level, or status as an employee at a given firm.
3. **Authenticator** – Data issued to an entity that provides access to restricted or protected systems. Examples of common authenticators are username/password combinations and access tokens that generate limited use codes.

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

5.1.1 Identities

Identities represent distinct entities within the ecosystem; parties wishing to interact with each other. Identities consist primarily of information that uniquely identifies an entity in a given context (e.g., a registered legal name and identifier for a business). For persons, identities demonstrate that the individual is who she/he purports to be.

Within the PCTF, **identity providers** are responsible for creating and managing digital identities over which they have scope. They perform functions that consist of processes to ensure that:

- an entity is known to be real and identifiable, not a fraudulent creation; and
- an entity is unique within a population (e.g., citizens, customers, corporations) so that multiple digital identities cannot be fraudulently created and used;
- the digital identity represents the entity to which it was issued.

These functions provide a foundation on which digital representations can be created; they enable the creation of a “record” or “account” for the entity. Other participants can create credentials and authenticators linked to this record.

Types of Identities

The PCTF defines two types of information to establish a digital identity:

Type	Description	Issued To	Issued By	Examples
Foundational	Establishes the existence and digital representation of real, legally recognized entities.	Persons, Organizations	Certain public sector agencies with a mandate to create and manage legally accepted identities (e.g., registrars, citizenship and immigration agencies).	A data set that attests the subject's identity, such as the digital equivalent of a birth certificate or articles of incorporation.
Contextual	Establishes identity and digital representations of entities in specific contexts or use cases. This type includes IDs that are self-issued or assigned.	Persons, Organizations , Machines	Public and private or non-profit identity providers.	Digital corporate ID, digital ID from a professional body. Social media identity, self-issued identity. In the case of machines, these could be digital identifiers assigned by manufacturers or intelligent agents

Processes Typically Performed by Identity Providers

Process	Description
Identity resolution	The establishment of the uniqueness of a subject within a program/service population through the use of identity information. A program or service defines its identity resolution requirements in terms of identity attributes; that is, it specifies the set of identity attributes that is required to achieve identity resolution within its population.

Identity establishment	The creation of an authoritative record of identity that may be relied on by others for subsequent programs, services, and activities.
Identity maintenance	The process of ensuring that identity information is as accurate, complete, and up-to-date as is required. Identity Maintenance also includes *identity notification* which is the disclosure of identity information triggered by a change in identity information, (e.g. a vital or a major life event) or an indication that identity information has been exposed to a risk factor. May be time-based or event-based.

5.1.2 Credentials

Credentials are digital representations that provide information about the attributes or properties of an entity. Credentials typically contain information beyond what is needed to identify a unique, individual entity. A credential includes one or more identifiers which may be pseudonymous, and attributes verified by the credential issuer.

A credential may be a simple construct that attests to a person’s age or a business’ registration status in a given province. They may also be more complex constructs that represent university transcripts, employment histories, or position within an organization. For persons, credentials help answer questions like “is this person legally permitted to purchase these goods online?” or “does this person meet the requirements needed to receive these government benefits?”.

Credentials are used by service providers and relying parties to have confidence in specific characteristics of that entity (e.g., age to purchase a financial product) are true. In some use cases, the existence of the credential and its use may provide a digital footprint or evidence of liveness that can assist identity proving and risk assessment and mitigation.

A credential is not synonymous with a username and password or similar mechanism used to control access to a managed system. In the PCTF context the username and password given to a person to access a specific website, for instance, is referred to as an *authenticator*.

Within the PCTF, **credential providers** are responsible for creating and managing credentials. They create and provide functions that consist of processes to ensure that:

- credentials are issued (or bound) to the correct subject;
- the credential is revoked or suspended as and when required; and
- information stored in the credential is current and accurate.

Depending on how the credential is stored and managed, credential providers may also be responsible for processes to ensure that:

- the credential can be disclosed as needed and according to specified conformance criteria;
- relying parties can verify the information contained in a credential;
- relying parties can verify credential status (e.g., whether or not the credential has been revoked or otherwise rendered invalid).

420 **Types of Credentials**

421 The PCTF defines two types of credentials, each providing a specific type of information:

421-a	**Credential Type**	**Description**
421-b	Attribute	A credential that provides one or more pieces of information about a single entity. Examples: A simple credential issued by a province that contains a single piece of information attesting to the entity’s age. A simple credential attesting to the entity’s security clearance level. A credential attesting to the fact that a certain mobile phone number is assigned to the entity’s handset. A more complex credential that is a university transcript consisting of data that identifies the courses a student has taken.
421-c	Relationship	A credential that attests to the fact that an entity is connected to, affiliated with, or otherwise related in some way to a second entity. Example: A credential issued by a corporate registrar attesting to the fact that a person is an officer of a corporation or credentials issued by the corporation to its personnel that prove they are employed by the firm. A delegation of authority is a particular type of relationship. These credentials attest to the fact that an entity has delegated certain rights, privileges, authorities, etc. to a second entity. Example: A simple credential attesting to the fact that a corporate officer has delegated financial authority to an entity.

422 **Processes Typically Performed by Credential Providers**

422-a	**Process**	**Description**
422-b	Credential issuance	The process during which a credential is created, assigned to a subject (i.e., a person, organization, application, or device), and optionally bound to one or more authenticators. Authenticators can be subsequently used to prove that a credential is referring to the same subject that was originally bound to the credential.
422-c	Identity-credential binding	The process of associating credentials to an attributed actor.
422-d	Credential maintenance	The process includes lifecycle activities such as updating credential details. This process is typically initiated by the subject but may also be initiated by a system administrator or automatically by the system.
422-e	Credential suspension	Transitions an issued credential to a suspended credential. This can be triggered by the subject (e.g. forgotten password) or the system (e.g., lockout due to successive failed authentications, inactivity, suspicious activity, etc.). A suspended credential is prohibited from being passed to a Relying Party, thereby ensuring that the subject is denied access.

Credential recovery	Transitions a suspended credential back to a usable state (i.e., an issued credential). The process may be triggered by the subject, system administrator, or automatically by the system.
Credential revocation	Ensures that a credential is permanently disabled or deleted. Once a credential is revoked, it can no longer be used. The process can be initiated by the subject, system administrator, or automatically by the system.
Credential authentication	Verifies that a subject has control over their issued credential.

5.1.3 Authenticators

Authenticators are data used to access managed or protected systems (e.g., a financial institution's website). An authenticator may be a simple username-password pair or a more complex object like an access token or biometric data.

In the context of the PCTF Model, the term "authenticator" is not synonymous with "credential".

Authenticator providers are responsible for creating and managing authenticators. They perform functions that ensure lifecycle management of the authenticator (including processes for issuance, suspension, recovery, maintenance, and revocation of authenticators).

Processes Typically Performed by Authenticator Providers

Process	**Description**
Authenticator issuance	The process during which an authenticator is created and assigned/bound to a subject (i.e., a person, organization, application, or device), and bound to one or more authenticators.
Identity-authenticator binding	The process of associating authenticators to an attributed actor.
Authenticator maintenance	The process includes lifecycle activities such as removing authenticators, binding new authenticators, and updating authenticators (e.g., password change, updating security questions and answers). This process is typically initiated by the subject but may also be initiated by a system administrator or automatically by the system.
Authenticator suspension	Transitions an issued authenticator to a suspended authenticator. This can be triggered by the subject (e.g., forgotten password) or the system (e.g., lockout due to successive failed authentications, inactivity, suspicious activity). A suspended authenticator is prohibited from being passed to a Relying Party, thereby ensuring that the subject is denied access.

Authenticator recovery	Transitions a suspended authenticator back to a usable state. The process may be triggered by the subject, system administrator, or automatically by the system. Examples include: • The subject correctly answers the security questions to reset a forgotten password • A system administrator releases an authenticator that was suspended due to inactivity • After 24 hours the system automatically releases an authenticator that was suspended due to excess failed authentication attempts

5.2 Using Digital Representations

For most people, proving identity, accessing an account, or demonstrating that certain criteria are met (e.g., residency, age, possession of a permit) is a necessary part of online interactions. Functions in this category concern the use of digital representations for these purposes.

The interactions that depend on trusted digital representations are often interactions between a relying party and a digital representations subject:

- **Relying party –** In this context, a relying party is the interaction participant that requires a digital representation for a valid purpose. Relying parties normally need information to identify subjects, check certain attributes, or grant access to a protected system. In many cases, the relying party is a government program, non-profit organization, or private firm offering services online to the public or a limited set of users. The relying party may be a business unit within a larger organization. The retail banking unit that manages an online account opening system for a large financial institution may, for instance, rely on information issued by an internal identity and security unit to interact with its customers.
- **Digital representation subject –** The entity represented by and to which data held in a digital object pertains (e.g., the person whose age can be verified using a credential). In this context, the digital representation subject is typically a person who wishes to conduct a transaction, access a system, or interact with a relying party in some other manner.

Given the diversity of technical, service, and business models that define digital interactions and how information about participants is incorporated into these interactions, the PCTF accepts that:

- other ecosystem participants may be involved in specific functions related to using digital representations**;**
- interactions may occur between digital representation subjects directly (i.e., in a peer-to-peer interaction without additional parties involved); and
- interactions may occur without direct involvement of the digital representation subject

The varied nature of these interaction models limits this document to an overview of fundamental processes involved in using digital representations.

5.2.1 Confirmation of a Digital Representation

The confirmation processes ensure that:

1. the identity of an entity is known with some degree of certainty; and
2. the information that is part of a digital representation is accurate, valid, or otherwise fit for purpose.

Process	**Description**
Identity validation	The confirmation of the accuracy of identity information about a subject as established by an authoritative party. It should be noted that identity validation does not ensure that the entity is using their own identity information (this is Identity Verification) – only that the identity information that the subject is using is accurate when compared to an authoritative record.
Identity verification	The confirmation that the identity information being presented relates to the subject who is making the claim. It should be noted that Identity Verification is a separate process from Identity Validation and may employ different methods and use personal information that is not related to identity. Different methods may be used (separately or in combination) such as: • Knowledge-based confirmation • Biological or behavioural confirmation • Trusted referee confirmation • Physical possession confirmation
Credential/authenticator authentication	This process establishes a level of confidence that an entity has control over a credential or authenticator issued to that entity.
Identity linking	The process of ensuring that the right subject is properly associated across different service delivery contexts. This process is dependent on authority and privacy constraints and may result in the association of an identity with a service assigned identifier, and/or, the mapping of multiple service assigned identifiers associated with an identity.
Identity presentation	The dynamic confirmation that a subject has a continuous existence over time (i.e., “genuine presence”). This can be used to ensure that there is no malicious or fraudulent activity (past or present) and to address identity spoofing concerns.

5.2.2 Consent for Digital Representation Use

These processes ensure that digital representation subjects understand which information in a digital representation is being used, for what purpose – and that they give their permission for its use where applicable.

Process	**Description**
Formulate notice	Produces a statement that describes what personal information is being collected; with which parties the personal information is being shared; for what purposes the personal information is being collected, used, or disclosed; how the personal information will be handled and/or protected; the time period for which the statement will be applicable; and under whose Jurisdiction/Authority the statement is applicable. This statement is presented to the subject (i.e., the natural person to whom the personal information in question pertains) in the form of a notice statement.
Request Consent	Presents the notice statement to the subject and providing a capability for the subject to provide consent or decline consent based on the contents of the notice statement, resulting in a consent decision.
Record Consent	Persists the notice statement and the subject's consent decision, to storage. In addition, information about the subject, the version of the notice statement that was presented, the date and time that the notice statement was presented, and, if applicable, the expiration date for the consent decision may be stored. Once the consent information has been stored, a notification on the consent decision made is issued to the relevant parties to the consent decision.
Manage consent	The Manage Consent process manages the lifecycle of consent decisions and consists of two sub-processes: 1. Review: The process to review consent involves making the details of a stored consent decision visible to the subject or to a reviewer. 2. Update: Updating a consent decision involves the subject establishing a revised consent decision from a previously stored consent decision. This could include the subject revoking the consent. This process results in an updated consent decision (which will require persisting via the Record Consent process).

5.3 Enabling Digital Identity Systems

The goal of the PCTF is to enable and support a Canadian digital identity ecosystem. Interoperation and collaboration combined with a responsible governance process among participants in a secure and privacy-enhancing environment is at the heart of such an ecosystem. To successfully meet this goal, the PCTF defines requirements and guidelines that establish a level of trustworthiness for processes carried out within the ecosystem. These processes are delivered over a combination of public, private, trusted and untrusted shared infrastructure: the devices, networks, software, and facilities that allow participants to develop, deploy, manage, and support the services they provide to their clients and the public.

The objective of the PCTF with respect to this infrastructure is to ensure the trust created at the function and process level is also present in the infrastructure that enables the digital identity ecosystem. This helps ensure that the infrastructure supports the delivery of trusted services and addresses challenges common to all participants.

To this end, the PCTF defines guidelines and standards for processes that **infrastructure providers** deliver to other participants. These processes, which fall into technical and operational infrastructure, include:

- physical and system security;
- data confidentiality, integrity and availability;
- incident reporting; and
- record keeping

5.3.1 Technical Infrastructure

These processes ensure the security and integrity of enabling infrastructure components.

Process	**Description**
Security	IT security practices designed to ensure the confidentiality, integrity, and availability of supporting infrastructure.
Data management	Processes and policies for the lifecycle management of digital representation data, including oversight of data collection, validation, storage, and accessibility on an on-going basis.
Audit and logging	Processes to establish and maintain a chronological record or records that provide evidence of events and activities of events (system, transaction, or otherwise) related to supported functions.
Technical standards	PCTF reference to relevant industry standards in support of specified functions.

5.3.2 Operations Infrastructure

These processes ensure that there are well-defined operational principles and practices for the digital identity ecosystem.

Process	**Description**
Risk management	Processes for the identification of direct or indirect risks to supported functions and related efforts to reduce or eliminate the likelihood of these risks occurring.
Records management	Processes that support typical record-keeping activities for supported functions. This includes classification, retention schedules, preservation, and disposition.

Incident and dispute management	Processes to identify, assess, and respond to events that adversely affect supported functions and (in the case of disputes) ecosystem participants – including efforts to reduce or eliminate the likelihood of the incident recurring.

6. Glossary of Terms

Terminology may vary depending on the context or sector where a term is used. The following list defines the key terms used in the context of this PCTF Model document.

Authenticator – The methods entities within the ecosystem use to access restricted or protected systems (e.g., a financial institution's website).

Credential – Information describing the attributes or properties of an entity.

Digital Representation – An electronic dataset that refers to any type of entity that can be subject to legislation, policy, or regulations within a context, and which may have certain rights, duties, and obligations.

Entity – Something that has separate and distinct existence and that can be subject to legislation, policy, or regulations within a context, and which may have certain rights, duties, and obligations.

Identity – Information about an entity that uniquely describes the entity within a given context.

Role – A set of functions and obligations that are assigned to a particular defined position within the context of the trust framework, such as "identity provider" or "relying party."

Subject – An entity to which a digital representation in an identity management system pertains.

User – A person accessing digital services or digital resources.