Pan Canadian Trust Framework Model Overview Discussion Draft Version 0.02

This discussion draft 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 discussion draft 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, please consider the following:

1. A glossary of terms will be shared in the near future and will be informed by this review.
2. Is the general structure and tone in the expected direction?
3. Is the scope too narrow, too broad, or appropriate, bearing in mind other components may address details out of scope for this document?
4. Do you agree with the specific terms as they are presented in the document?
5. Do you agree with "Digital Identity" to refer to the information of concern? Agree or suggest a new term.

Table of Contents

1. Introduction

As service delivery becomes entirely digital, individuals, governments, and businesses realize a need to trust information about those with whom they interact; that the user at the other end of a connection is who he or she claims to be, or that information about that user is correct. Users and service providers also need to know that this information is protected as it travels across networks and organizational boundaries. This is particularly true in high-value or high-sensitivity transactions that are currently difficult to conduct digitally. Such transactions include purchasing real estate, submitting a response to a request for proposals, or managing government benefits on behalf of an elderly parent.

In response, governments and industries around the world are developing technology and policy frameworks to create trusted environments online. Commonly known as trust frameworks, these frameworks enable one organization to rely with confidence on business and technical functions performed by other organizations. In so doing, trust frameworks help enable interactions between and across various networks and organizations. Many of the financial systems in use today, like credit and debit cards, 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.

In the digital identity domain, a trust framework is a set of auditable business and technical requirements for functions that identify, authenticate, and authorize users accessing services and resources from multiple organizations. In this sense, a trust framework enables trust in information about participants and, by extension, facilitates trustworthy digital interactions. Information about these participants exists as digital identities.

The Pan-Canadian Trust Framework (PCTF) is a trust framework for digital identities in Canada. It consists of modular components that establish standards and guidelines for the delivery of trusted digital services to the public and private sectors. The Privacy 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 privacy processes ensure that identity systems follow privacy-respecting practices, ensuring personal information is properly collected, protected and maintained.

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

1.1 About this Document

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

This document also outlines the functional areas of primary concern to the PCTF. The outline (provided in section 4) provides a general sense of the information that the PCTF is concerned with and the various processes involved in creating, managing, and using that information. Individual PCTF component documents provide detailed descriptions of the functions highlighted in this document.

The audience for this document includes:

- members of the digital identity community – as key stakeholders and contributors to the PCTF;
- digital identity technology and service providers – to understand where they fit in the PCTF and to help define and assess requirements for their products and services; and
- users of digital identity services (e.g., service providers, and individual users) – to assess the value of employing trusted digital identity solutions and processes when interacting online.

2. About the PCTF

Development of the PCTF is a collaborative effort between The Digital ID and Authentication Council of Canada (DIACC) and the Pan-Canadian Identity Management Sub-Committee (IMSC) of the Joint Councils of Canada. DIACC is a non-profit neutral forum. The Joint Councils of Canada are a forum consisting of the Public Sector Chief Information Officer Council (PSCIOC) and the Public Sector Service Delivery Council (PSSDC).

Individuals and organizations residing or doing business in Canada are the ultimate beneficiaries of the trusted environment that results from standardization and conformance with 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 reflects and supports this aspect of digital services as a trust framework providing consistent and auditable processes for the creation, management, and use of digital identities.

However, to be successful, the use of information about participants must scale beyond a limited number of relationships. It must scale beyond limited one-off integrations. Digital identities must work 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.

A high degree of interoperability requires mutual trust. 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, credentials, and the identity management systems needed to administer them all; and
- hampered modernization efforts that foster innovation and improve service experience, efficiency, and effectiveness.

Canadians expect their digital identity infrastructure to operate with transparency, ensuring fairness for all. Furthermore, Canadians 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-respecting Canadian digital identity ecosystem.

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 regardless of where they live or work.

The PCTF supports development of a Canadian identity ecosystem by:

- ensuring the Canadian digital identity ecosystem is trustworthy and encourages a fair, innovative, and competitive environment;
- supporting inclusion of participants offering a broad range of services;
- identifying applicable existing policy and technology standards that meet the needs of ecosystem stakeholders; 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 and user-centric approach to digital identity can be achieved by defining agreed upon standards that are implemented and assessed in a consistent manner. Accordingly, objectives of the PCTF focus on ensuring the trustworthiness of the Canadian digital identity ecosystem by:

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

2.4 Scope

The PCTF establishes a standards framework within which innovative solutions can be developed, measured and recognized. It defines requirements and conformance criteria necessary for digital identity ecosystem participants to interact with assurance.

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

2.5 Guiding Principles

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

1. **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".
2. **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. **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 are informed about the potential benefits and consequences of digital identities.
4. **Support robust, secure, scalable solutions** – Canada's digital identity ecosystem must be sufficiently robust to ensure security, availability, and accessibility at all times.
5. **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.
6. **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.
7. **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.
8. **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.
9. **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.
10. **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.

3. Core Concepts

The PCTF is based on a small number of core 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 information about participants in digital interactions.

These core concepts can be summarized as follows:

- participants in the digital identity ecosystem generate, process, and/or store **digital identities**;
- when processing digital identities, participants assume one or more **roles** in the ecosystem;
- each role performs a number of functions (made up of detailed processes); and
- common **conformance criteria** can be defined to assess the trustworthiness of key processes – allowing them to be designated *trusted processes.*

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

3.1 Digital Identities

The goal of the PCTF is to support development of a digital identity ecosystem that engenders trust and confidence for Canadians and the service providers with which they interact digitally. At the core of such an ecosystem is the information about participants in an interaction. This information makes up their respective digital identities.

In the PCTF context, a digital identity is an electronic dataset that identifies an entity and/or describes characteristics of that entity. Digital identities consist of one or more types of information:

1. **Identity** – Information that makes it possible to identify a unique participant (e.g., personally identifiable information), either on its own or with supporting related information. Examples include names, dates of birth, birth registrations, etc.
2. **Authenticator** – Data issued to a participant by a system administrator that provides access to restricted or protected systems. Examples of common authenticators are username/password combinations and access tokens that generate limited use codes.
3. **Credential** – Information describing attributes and properties of a participant. This information may exist on its own (e.g., as a claim within a credential that contains no personally identifiable information, only a unique string identifier) or be related to personally identifiable information. Examples include education levels (i.e., a university degree in engineering), permission to operate a vehicle (i.e., a driver's license), income level, or status as an employee at a given firm.

3.2 Participant Roles

The information that makes up a digital identity goes through a lifecycle that begins with creation, proceeds to active use (during which the data may change, credentials may be added or removed, etc.), and then to archival and, in some cases, destruction. Trust is created during the execution of key functions throughout this lifecycle – and the PCTF defines standards and guidelines for these functions.

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

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

Ecosystem participants that perform these key functions in the information lifecycle of digital identities assume one or more roles that are defined as follows in the PCTF context.

Category	Role	Description
Create and manage digital identities	Identity providers	Participants that create and manage identities. Sometimes referred to as identity service providers. In some cases, the user is the creator and manager of its own identity.
	Credential providers	Participants that create and manage credentials that cannot be used on their own to identify a participant. Sometimes referred to as attribute providers.
	Authenticator providers	Participants that create and manage authenticators. Sometimes referred to as credential service providers. But are not the same as PCTF Credential Providers. See section 4.1.3 for details.
Use digital identities	Relying parties	Participants who rely on identity information created and managed by other participants to conduct digital interactions – primarily with digital identity owners.
	Digital identity owners	The entity to which digital identity information is issued or the information is about. This information is shared with other participants, primarily relying parties, during digital interactions when required.
Enable digital identity systems	Infrastructure providers	Participants that provide the physical and electronic infrastructure needed to enable digital transactions.
	Assessors	Participants accredited to assess another participant's compliance with the PCTF.

Given the fluid nature of these roles and associated functions, The PCTF recognizes that:

- Intended ecosystem participants include public, commercial, non-profit, and other types of organizations that provide, consume, or rely on identity-related services and information.
- Ecosystem participants will in many situations assume one, multiple, or all roles and associated functions. For example, a government registrar may issue a digital identity to a business (acting in the role of identity provider), but also request verification of the identity issued by a a different registrar to persons associated with that business (acting as a relying party). Or, a business may create and mange a digital identity consisting of an identifier for an employee, a credential attesting to the employee's security level within the firm and associated systems, and an authentication token (acting as identity, credential, and authenticator provider).
- Ecosystem participants may specialize in one specific role (or process within that role) or fall generally into multiple roles. For example, a private business may focus exclusively on developing and selling technology to issue and revoke credentials to users while

another provides a digital wallet to help users manage their credentials while another provides browser-based technology to manage authenticators.

As a trust framework intended for broad adoption, the PCTF also 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.

Category	Role
Govern PCTF	• Digital Identity and Authentication Council of Canada (DIACC) • Pan-Canadian Identity Management Sub-Committee (IMSC) of the Joint Councils of Canada

3.3 Conformance Criteria

The requirements, specifications, recommendations, guidelines, and other items that comprise a standard for specific processes are referred to as conformance criteria. Participants can use these criteria to inform design and development of their products and services.

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

- Existing standards and specifications may be incorporated into the PCTF by reference. This ensures broad compatibility and reduces duplication and overlap of content and technical specifications. For example, as part of its conformance criteria, a PCTF component document may recommend adoption of relevant standards for user authentication published by the World Wide Web Consortium (W3C).
- 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.

Also in keeping with the guiding principles, 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.

3.4 Trusted Processes

A trusted process is a business or technical activity (or set of such activities) that transforms an input condition to an output condition. For example, a trusted process may consist of the assignment of a unique identifier to one and only one subject. Various controls are to be in place to ensure that this process has integrity, and that other trusted processes or services can rely upon this process.

Trusted processes are crucial to ensuring the integrity of access to digital services, to the overall integrity of the digital supply chain, 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 and certification process.

A business or technical process that is designated as a trusted process is assessed and certified according to conformance criteria defined in PCTF components.

4. Functional Outline

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

4.1 Creating and Managing Digital Identities

Functions in this category involve proving or checking the identity or characteristics of a real entity (e.g., a person) and creating a digital identity for that entity. Once a digital identity 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 information remains current and accurate.

The PCTF recognizes that digital identities can be created and managed for entities other than people. Digital identities can be created and managed for:

1. **Persons** – An individual, natural person. Examples of persons include residents of a jurisdiction (country, province, etc.), the customers of a business, and private individuals without reference to a government register.
2. **Legal entities** – An entity whose existence is established by legal statute or convention. Examples of legal entities include businesses (including sole proprietorships and partnerships), government agencies, registered charities, and similar types of organizations. Typically, persons act on behalf of a legal entity as business and other organizations and are not, strictly speaking, autonomous identities in their own right.
3. **Machines** – Software (e.g., apps) and hardware (e.g., smartphones) that can be uniquely identified. Typically, machines act on behalf of a person or legal entity and are not autonomous identities in their own right. Future technical developments may see the creation of machines that exhibit some level of autonomy.

Given the variety of technical, service, and business models that define digital interactions and how information about participants is incorporated into these interactions, the roles of identity, credential, and authenticator providers may be performed by multiple participants in a given context.

4.1.1 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 help answer the question “is this a real, unique and known individual?”

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

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

These functions provide a foundation on which an identity for a person can be created; they enable the creation of a "record" or "account" for the entity within a system. Other functions can create credentials and authenticators linked to this record.

Types of Identities

The PCTF defines three types of digital identities:

Type	Description	Issued To	Issued By or Source
Foundational	Establishes the existence and digital representation of real, legally recognized entities.	Persons, legal entities	Certain public sector agencies with a mandate to create and manage legally accepted identities (e.g., registrars, citizenship and immigration agencies). Example: A data set that attests the owner's identity, such as the digital equivalent of a birth certificate or articles of incorporation.
Functional	Establishes identity and digital representation of real, legally recognized entities in specific contexts or use cases.	Persons, legal entities	Public and private identity providers. Example: Digital corporate ID.
Auxiliary	Establishes the identity of any entity with varying levels of trust and may link back to foundational and functional identities. Information may be self-asserted. Usually have lowest level of trust of the three types of digital identity.	Any entity	Public and private identity providers. Example: Social media identity, self-issued identity.

Identity Provider Typical Functions

Function	Description
Source establishment	A preparatory activity undertaken to determine what evidentiary information is used to validate and/or verify the person and the assurance of those sources. A typical identity provider will use a range of sources in order to support the needs of different entity types and to meet target trust levels.

Identity resolution	Establishment of the uniqueness of an entity within a population using source information. The identity provider defines identity resolution requirements in terms of identity data; it specifies the set of identity data that is required to achieve identity resolution within its population.
Identity establishment	Creation of a record of identity on which other participants can rely for subsequent identity information creation and service interactions.
Identity linking	Resolving identity information that exists in multiple sources is for a single entity.
Identity issuance	Creation of evidence of identity issued to the identified entity. Other participants can rely on this evidence for subsequent identity verification and validation during various interactions.
Identity maintenance	On-going upkeep of a digital identity, such as dealing with events that affect previously performed Identity Validation and Identity Verification. This could include the evidence changing, expiring or being revoked. It could also include evidence becoming stale due to the passage of time.

4.1.2 Authenticators

Authenticators are the methods entities within the ecosystem use to access managed 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 collected from a sensor.

Within the PCTF, **authenticator providers** are responsible for creating and managing authenticators. They perform functions that consist of processes that ensure:

- life-cycle management of the authenticator including issuance, suspension, recovery, maintenance, and revocation; and
- binding of the authenticator to an entity.

Types of Authenticators

The PCTF defines two types of authenticators:

Authenticator Type	Description
Login	Data and associated functions to authenticate a user attempting to access a system.
Cryptographic Signature	Data and associated functions for asserting identity and binding it to a document, message, or other item.

These two types of authenticator are not mutually exclusive:

- A login process may be used to protect access to a cloud-based cryptographic key used for digital signing
- Transaction or session information may be digitally signed as part of a login or step-up process.

Authenticator Provider Typical Functions

Function	Description
Authenticator issuance	An enrolment function, during which an authenticator is created and bound to an entity. Authenticator details may be automatically assigned during this process, provided by the subject entity, or provided by a third-party.
Authenticator maintenance	Life-cycle activities such as binding new authenticators, removing authenticators, and updating authenticators (e.g. password change, updating security questions and answers).
Authenticator recovery	A means to transition an inaccessible authenticator to a usable state. The process may be triggered by a subject entity, authenticator provider, or automatically by the system.
Authenticator revocation or suspension	Changing an issued and usable authenticator to an unusable authenticator. This function may be initiated by the subject entity, the authenticator provider, or automatically by the system. A revoked or suspended credential is prohibited from being passed to other participants, ensuring the subject entity is denied access to other systems.

4.1.3 Credentials

Credentials represent information about or the properties of an entity beyond the information that identifies a unique individual entity. 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?"

A credential is not synonymous with a username and password or similar mechanism used to control access to a specific system. In the PCTF context the username and password given to a user to access a specific website, for instance, is referred to as an *authenticator*. Credentials can support online authentication and authorization processes. Highly trusted credentials are linked back to or include identity information about their subjects (e.g., a university transcript will identify the person to whom it refers).

The entity to which the credential applies (i.e., the *subject*) typically shares one or more credentials as a way to demonstrate entitlement to a service or offering. For this to be a trusted process, the credential typically includes:

- information about the subject (e.g., name);
- a means to verify that the information pertains to the subject in question (e.g., unique identifier for the subject);
- a means to verify that the information was established by a known and trusted source (e.g., unique identifier for the issuer); and
- a means to show that the information is still valid (e.g., cryptographic key information).

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

- credentials are issued (or bound) to the correct subject;
- credentials are stored securely and appropriately;
- 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 that ensure:

- the credential can be disclosed at the request of the subject or in accordance with relevant legal frameworks;
- 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).

Types of Credentials

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

Credential Type	Description
Attribute	A credential that provides one or more pieces of information about a single entity. Example: A credential issued by a province that contains a claim attesting to the subject's age.
Delegation	A credential that attests to the fact that an entity has delegated certain rights, privileges, authorities, etc. to a second entity. Example: A digital power of attorney for property issued by a government agency.
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 (but which does not extend to include delegations of any authority between the two). Example: A credential issued by a corporate registrar attesting to the fact that a person is an officer of a corporation or a credential issued by the corporation to its personnel that prove they are employed by the firm.

Credential Provider Typical Functions

Function	Description
Source establishment	A preparatory activity undertaken to determine what evidentiary information is used to ensure credentials are issued to valid recipient entities.
Credential issuance	Creation of evidence of the credential issued to the subject entity. Other participants can rely on this evidence for subsequent identity verification and validation during various interactions.
Credential storage	Credential providers can issue credentials directly to subject entities (i.e., the subject holds the credential in a location of their choosing). Alternatively, the credential provider may store the credential on behalf of the subject and provide associated functions for managing and using that credential.

Credential maintenance	On-going upkeep of a credential, such as dealing with events that affect the validity of the credential. This could include events that make the subject ineligible to hold a given credential (e.g., the person is no longer able to drive a car), changes to credential details (e.g., a person has taken a new role in an organization), or a validity period has lapsed (a permit has expired).
Credential revocation and suspension	Specific functions that the credential provider can perform as part of credential maintenance in response to changes in credential details and validity.
Credential recovery	A means to transition an unusable credential to a usable state.

4.2 Using Digital Identities

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 identities for these purposes. The PCTF is particularly concerned with helping ecosystem participants ensure a high degree of certainty and trust in digital identities. This is critical to ensuring digital delivery of high-value services like applying for a passport, opening a bank account, or transferring asset ownership (like real estate).

The transactions that depend on trusted digital identities are primarily interactions between a relying party and a digital identity owner:

- **Relying party** – In this context, a relying party is the interaction participant that requires digital identity information for some purpose. Relying parties normally need identity information to identify users, check their credentials, or grant access to a system using an authenticator. In many cases, the relying party is a government program 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 a digital identity information issued by an internal identity and security unit to interact with its customers.
- **Digital identity owner** – In this context, the digital identity owner is usually the user who wishes to conduct a transaction, access a system, or is the subject of the identity information (e.g., the subject of a proof of age credential) – but the user may also have a credential that allows them to use information on behalf of others. Since service delivery is often dependent on information commonly found in a digital identity, the owner either provides the required information directly to the relying party or consents to another party sharing the information with the relying party.

Given the variety of technical, service, and business models that define digital interactions and how information about participants is incorporated into these interactions, other ecosystem participants may also be involved in specific functions related to using digital identities. **This is particularly true of identity providers and credential providers**.

The varied nature of these transaction models limits this document to an overview of fundamental functions involved in using digital identities. Generally, these functions are concerned with the following:

- confirmation of a digital identity; and
- consent for digital identity use.

4.2.1 Confirmation of Digital Identity

These functions 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 identity is accurate, valid, or otherwise fit for purpose.

Function	Description
Identity validation	Confirmation of the accuracy of a digital identity about an entity as established by an authoritative party. “Identity validation” is equivalent to the term “identity information validation.” Identity validation does not ensure that the person is using their own digital identity (this is identity verification) – only that the digital identity being used is accurate and current.
Identity verification	Confirmation that the digital identity being used relates to the entity using the identity. Identity verification is a separate function from identity validation. This function may employ different methods and use personal information that is not related to identity.
Authentication	This function establishes a level of confidence that an entity has control over an authenticator issued to that entity and that the authenticator is currently valid (i.e., not suspended or revoked).
Authenticated session initiation	An authenticated session enables a persistent interaction between a digital identity owner and an end-point while removing the need to continuously repeat authentication processes between interactions. This trusted process is not necessary in all circumstances but may be required to satisfy certain use cases such as federation and single sign-on.

4.2.2 Consent for Digital Identity Use

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

Function	Description
Formulate notice	Establishes a statement that describes what identity information is being collected, used, or disclosed; what the purpose is for the collection, use, or disclosure of the information; to whom the information will be disclosed; how the information will be handled and/or protected; the time period for which the notice will be applicable; and under whose jurisdiction or authority the notice is applicable.

Request Consent	Ensures that it is the information owner who is performing the action to indicate authority to make the consent decision. This will typically involve identifying and authenticating the information. The function to request consent of a subject includes presentation of a notice to the owner and providing a capability for the owner to impart a decision to provide consent or decline consent to the information in the notice, resulting in a consent decision.
Record Consent	This function involves storing a record of the notice conditions and the owner's consent decision. Examples of notice conditions that may be stored include pertinent information about the owner, the date/time of notice presentation, and the version of the notice presented. Examples of consent decision conditions to be stored include the notice conditions, plus the consent decision made by the owner, and, if applicable, the expiration date for the consent. Once the consent decision has been stored, a notification on the consent decision made is issued to the relevant parties to the consent decision.
Manage consent	The function is required to manage the life-cycle of consent decisions. This includes renewal of consent and revoking of consent.
Review	This function involves making the details of a stored consent decision visible to reviewers.

4.3 Enabling Digital Identity Systems

The goal of the PCTF is to enable and support the establishment of a Canadian digital identity ecosystem. Interoperation and collaboration between participants in a secure and privacy-respecting 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 identity-related functions carried out within the ecosystem. These functions are delivered over a combination of public, private, and 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 digital identity systems. This helps ensure that the infrastructure supports delivery of trusted digital identity services, and addresses challenges common to all participants.

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

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

4.3.1 Technical Infrastructure

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

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

460 ### 4.3.2 Operations Infrastructure

Function	Description
Risk management	Functions for the identification of direct or indirect risks to supported digital identity processes and related efforts to reduce or eliminate the likelihood of these risks occurring.
Records management	Functions that support typical record-keeping activities for supported digital identity functions. This includes classification, retention schedules, preservation, and disposition.
Incident management	Functions to identify, assess, and respond to events that adversely affect supported digital identity functions – including efforts to reduce or eliminate the likelihood of the incident recurring.

461