Pan-Canadian Trust Framework Model

Document Status: Final Recommendation V1.0

In accordance with the DIACC Operating Procedures, a Final Recommendation is a deliverable that represents the findings of a DIACC Expert Committee that have been approved by an Expert Committee and have been ratified by a DIACC Sustaining Member Ballot.

This document was developed by DIACC's Trust Framework Expert Committee with input from the public gathered and processed through an open peer review process. It is anticipated that the contents of this document will be reviewed and updated on a regular basis to address feedback related to operational implementation, advancements in technology, and changing legislation, regulations, and policy. Notification regarding changes to this document will be shared through electronic communications including email and social media. Notification will also be recorded on the Pan-Canadian Trust Framework Work Programme. Changes to this document that may affect certification and Trustmark status will be defined in the Pan-Canadian Trust Framework Assessment component.

Table of Contents

Pan-Canadian Trust Framework Model **1**
1 Introduction **4**
1.1 About this Document **4**
2 About the PCTF **5**
2.1 Context **5**
2.2 Goal **6**
2.3 Objectives **6**
2.4 Scope **7**
2.5 Guiding Principles **7**
3 Structure of the PCTF **8**
3.1 PCTF Components **8**
3.1.1 Model 9
3.1.2 Glossary 9
3.1.3 Assessment 9
3.1.4 Verified Person 10
3.1.5 Verified Organization 11
3.1.6 Credentials: Relationship and Attributes 12
3.1.7 Authentication 13
3.1.8 Notice and Consent 13
3.1.9 Infrastructure: Technology and Operations 14
3.1.10 Privacy 14
3.2 Conformance Criteria **15**
3.3 Trusted Processes **16**
3.4 PCTF Profiles **17**
4 Key Concepts **17**
4.1 Digital Representations **17**
4.2 Participant Roles **18**
4.3 Governance Roles **20**
5 Functional Outline **20**
5.1 Creating and Managing Digital Representations **20**
5.1.1 Identities 20
5.1.2 Credentials 22
5.1.3 Authenticators 24
5.2 Using Digital Representations **25**
5.2.1 Confirmation of a Digital Representation 26

5.2.2 Consent for Digital Representation Use 27
5.3 Enabling Digital Identity Systems 28
5.3.1 Technical Infrastructure 29
5.3.2 Operations Infrastructure 29
6 Revision History 31

1 Introduction

As service delivery becomes increasingly digital, individuals, governments, businesses, and other types of organizations realize a need to trust information about those with whom they interact; that the person (or other type of entity) at the other end of a connection is who he or she purports to be, or that information that person presents 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 digitally captured as evidence in legal transactions. 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, using passports online, purchasing controlled goods online, or managing government benefits on behalf of an elderly parent.

In response, public and private organizations 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 a few privileged 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 an economic benefits focused set of resources that are developed in collaboration in the Digital ID & Authentication Council of Canada's (DIACC) Trust Framework Expert Committee (TFEC), published by the neutral governance of the DIACC, and benefiting from the broad input of the economic sector and from Canada’s federal, provincial, and territorial representatives of the Joint Councils Identity Management Subcommittee (IMSC). For more information about the DIACC, see www.diacc.ca.

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 can lower development and service delivery costs. More important, though, it 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 provides an overview of the surrounding context and outlines the goals and objectives of the PCTF.

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 this digital identity information.

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

The audience for this document includes:

- private and public sectors members of the digital identity community (including regulatory and standards bodies) – as key stakeholders and contributors to the PCTF;
- providers of digital identity technology and services – 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;
- digital identity innovators and researchers – who can alleviate problems by proposing different approaches; and
- consumers and the organizations that serve them online – 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.

Interoperability, particularly in an online environment that expects immediacy and flexibility, requires quick establishment of mutual trust. 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;
- hampered modernization efforts that foster innovation and improve service experience, efficiency, and effectiveness; and
- created a risk that if Canada does not lead in this domain it will need to adopt foreign solutions and the associated negative economic impact.

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—for all sectors of 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 the existence of analogue processes is also likely.

To support development of a Canadian Digital Identity Ecosystem, the PCTF adopts a pan-Canadian approach to digital identity. This approach is founded on broad-based agreement on the principles outlined herein and the standards provided or referenced in the PCTF components to:

- develop solutions that put Canadian social, legal, and economic perspectives first; and
- serve the needs of all Canadians.

The PCTF supports development of a Canadian Digital Identity Ecosystem by:

- ensuring the Canadian Digital Identity Ecosystem is trustworthy – by putting control in the hands of consumers, preserving technical security and reliability, and encouraging a fair, innovative, and competitive environment for participants;
- focussing on transparency and privacy regarding usage and disclosure of personal information – by viewing privacy as relevant to all PCTF components;
- supporting inclusion of participants offering a broad range of services – by remaining technology neutral;
- adopting and adapting existing conventions – by identifying applicable existing policy and technology standards for the ecosystem; and
- maintaining a forward-looking perspective – by looking for future areas of 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 and profiles 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 accessing digital services or digital resources must trust the system at all times. 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 and users 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 participants 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 participants adhere to the Trust Framework requirements.
10. **Minimize data transfer between sources and avoid creation of new or expanded 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 (thereby reducing creation of so-called "information honeypots").

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.

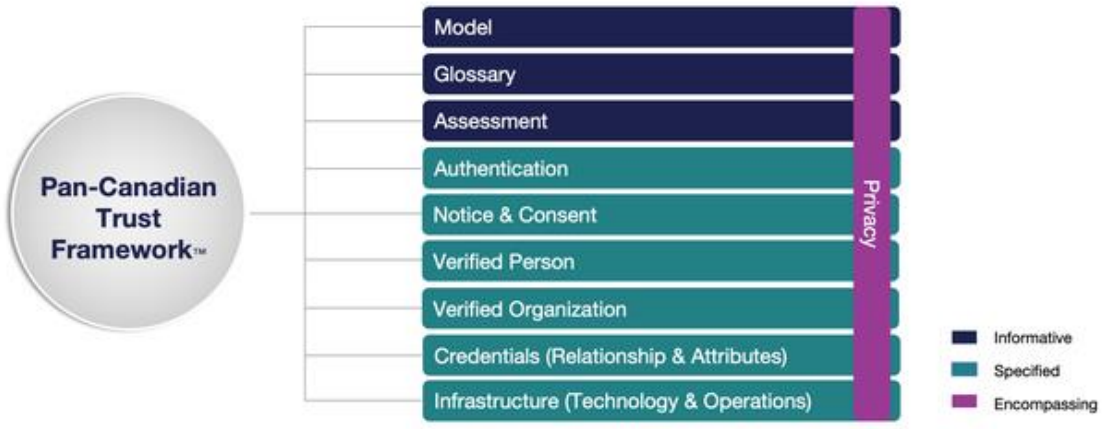

Figure 1. PCTF Components

Figure 1 is an illustration of the components of the draft PCTF. The focus of the PCTF components is to specify a common baseline of conformance criteria and trusted processes. DIACC stakeholders can extend and refine the baseline by defining PCTF profiles.

3.1.1 Model

This document, the PCTF Model Overview, describes the PCTF's goals and objectives, a high-level model outline of the PCTF, and contextual information.

3.1.2 Glossary

The PCTF Glossary provides definitions and examples for terms that appear across DIACC PCTF documentation. The objective of the PCTF Glossary is to ensure all stakeholders have a shared and consistent understanding of terms used in the context of the PCTF. As terms and usage can vary across industry, the glossary is recommended reading for anyone wanting a strong baseline understanding of the PCTF.

The content of the PCTF Glossary is:

1. **Terms** – The words or phrases that appear frequently and that are used with a specific intent (i.e., not their everyday English meaning) in the PCTF documentation
2. **Definitions** – A statement that provides the accepted and precise meaning of the associated term in the PCTF context
3. **Examples** – Examples or non-examples may be included to help clarify the intended meaning of a term; the examples provided are not intended to be an exhaustive list.
4. **Synonyms** – Terms with same or similar meaning used in other communities of interest

3.1.3 Assessment

The PCTF Assessment component describes the operation of the PCTF compliance certification program and the roles and responsibilities of stakeholder actors during the assessment and certification process. Specifically, this includes:

1. The roles and primary responsibilities of the organizations responsible for assessment and compliance:
    1. Certifying Authority
    2. Trustmark Issuer
    3. Accredited Assessor
    4. Certification Candidate
2. Within the identified organizations, a breakdown of pro forma roles and responsibilities within each of those organizations
3. High level descriptions of assessment methods and procedures, and their application
4. Certification program procedures and norms such as:
    1. Certificate issuance, publication, and maintenance
    2. Certification renewal procedures
    3. Assessment appeals procedures

This scope of this PCTF component does not include:

1. The internal processes of the Certification Candidate related to certification processes. Internal preparation for, and response to, Conformance Profile assessment procedures will vary based on the Certification Candidate's established internal governance and management processes. However, the core touchpoints and requirements are governed by the PCTF Assessment Component.
2. Assessment and Compliance Criteria for individual PCTF profiles. Individual PCTF Profiles provide specific criteria on certification when and where necessary.

3.1.4 Verified Person

The PCTF Verified Person component specifies processes and conformance criteria used to establish that a natural person is real, unique and identifiable. This is a key ingredient in ensuring a digital representation of a person is properly created, used exclusively to represent that same person, and can be relied on to determine if the person should receive valued services and to carry out transactions with trust and confidence.

The Verified Person component of the PCTF defines processes and specifies Conformance Criteria for:

1. **Verifying a person** - The processes that ensure the digital identity of a Person is an accurate representation of that Person and can be relied on for digital service delivery and digital transactions. A Verified Person is a real, unique and identifiable human being at the moment of Verification; and within the PCTF context such a person can be subject to legislation, policy, or regulations within a context. These processes ensure that a Person has been properly verified, and that they are the Person who initiated, directly or through a legally authorized representative, the request for a service or a transaction.
2. **Creating a trusted digital identity for a person** - The processes used to establish and maintain a digital record for a Verified Person in order to uniquely distinguish them from other Persons. The processes ensure that a digital record of a Person is properly created, used exclusively by that same Person either directly or aided by their legally authorized representative, and can be relied on for online transactions. This is also referred to as a Verified Person record.

The scope of the PCTF Verified Person Component includes:

1. Creating contextual identity evidence at an authoritative party
2. Relying on foundational identity evidence to verify a person
3. Relying on contextual identity evidence to verify a person
4. Levels of assurance 1-3 for identity; Level 4 use cases are currently out of scope but will be considered for future versions
5. Creating, updating, and managing a Verified Person record (i.e., a trusted digital representation)
6. Actors include Canadian federal, provincial and territorial governments and Canadian / PCTF compliant organizations as authoritative parties for identity evidence

The scope of the PCTF Verified Person Component does not include:

1. Creating foundational identity evidence. The establishment and maintenance of foundational identity evidence is the exclusive domain of the public sector, specifically

the Vital Statistics organizations of the provinces and territories, and Immigration, Refugees, and Citizenship Canada.
2. Using international governments or organizations as the only authoritative source for identity evidence to verify a Person. international governments may be referenced indirectly to establish foundational or contextual sources of identity. Use cases that rely only on international evidence of identity may be considered in later versions of PCTF.
3. Verifying non-identity attribute information. The Verified Person processes do not establish any particular information about the Person, only that the Person is real, unique and identifiable in a given context. Other personal information or attributes such as address of residency may be required to deliver a service. Verification of attributes not required for verifying a person's digital identity is outside the scope of this component; please refer to the PCTF Credentials (Relationships & Attributes) component.

3.1.5 Verified Organization

The purpose of the PCTF Verified Organization component is to specify Trusted Processes and associated Conformance Criteria that establish an Organization exists, is real, unique, and identifiable. Once a process is certified as conforming to the associated Conformance Criteria it becomes a trusted process which then can be relied on by other participants in a Digital Identity Ecosystem.

The PCTF Verified Organization component defines processes and specifies Conformance Criteria for:

1. **Establishing and verifying the Identity of an Organization** - This includes processes to ensure that an Organization has been properly verified as the expected participant in a given interaction. An Organization that no longer exists as a legal entity may still have a digital identity with an attribute indicating its status.
2. **Creating a trusted digital representation (i.e., a digital Identity) for an Organization** - These include processes to establish and maintain a digital representation for a verified Organization.

This PCTF component focuses those Trusted Processes that establish the Identity of the Organizations and the ongoing management of associated digital Identities. This includes:

1. Organizational Identity Establishment
2. Organizational Identity Issuance
3. Organizational Identity Resolution
4. Organizational Identity Validation
5. Organizational Identity Verification
6. Organizational Identity Maintenance
7. Organizational Identity Linking

The scope of this PCTF component does not include:

1. International governments or Organizations as authoritative sources for Identity evidence to verify an Organization. They may be referenced indirectly to establish foundational or contextual sources of Identity.

2. Processes by which stakeholders validate that individuals representing Organizations have the authority to do so.
3. Ownership structure of an Organization and the relevant conditions and processes for granting accessing to services and systems (private or public sector).

3.1.6 Credentials: Relationship and Attributes

This PCTF component specifies conformance criteria that Ecosystem Participants can use to assess the degree to which the ecosystem protects the use of digital Credentials. The scope of this component includes features of the digital Credential lifecycle and focuses on ensuring transparency and auditability as the primary methods for building trust across the Entities involved. Specific items deemed in or out of scope are described in the following sections.

In scope for this PCTF component are Credentials that:

1. Contain or provide information about a Subject (e.g., digital proof of educational qualifications) and an Issuer
2. Contain or provide information about the relationship between two Entities (e.g., digital proof that a person is an employee of a business)
3. Are issued by an Issuer to a Subject that is not the Issuer
4. Contain information one Entity provides about or to another Entity
5. Describes relationships between one or more Subjects and their relationships to one or more other Entities

Regardless of Credential content or the connection between an Issuer and a Subject, the scope of this component includes:

1. Issuance of Credentials to Subjects
2. Information that increases the trustworthiness of Credentials
3. Guidance on protecting the integrity and accuracy of Credential information
4. Direction on managing compromised Credentials

Verification and validation of unique, real, and identifiable Entities are out-of-scope for this component. Those processes, and the creation and use of Identity Information upon which they depend, is covered in the PCTF Verified Person Component and the PCTF Verified Organization components.

Also out-of-scope for this PCTF component are the following:

1. Issuance of a Credential by multiple Issuers
2. Rules and policies governing who can obtain a specific credential or specific type of credential (e.g., requirements to obtain a license to drive in a given jurisdiction)
3. Processes for assessing qualification or eligibility for a specific credential or type of credential (e.g., testing of new drivers), notwithstanding requirements to provide documentation of such processes
4. Acceptance of a credential for a given purpose (e.g., whether or not a driver's license is accepted as proof of address)

3.1.7 Authentication

The purpose of the PCTF Authentication Component is to assure the on-going integrity of login and authentication processes by certifying, through a process of assessment, that they comply with standardized Conformance Criteria. The Conformance Criteria for this component may be used to provide assurances:

1. That Trusted Processes result in the representation of a unique Subject at a Level of Assurance that it is the same Subject with each successful login to an Authentication Service Provider
2. Concerning the predictability and continuity in the login processes that they offer or on which they depend

The PCTF Authentication Component defines:

1. A set of processes that enable access to digital systems
2. A set of Conformance Criteria for each process that, when a process is shown to be compliant, enable the process to be trusted

3.1.8 Notice and Consent

The PCTF Notice and Consent component specifies conformance criteria that define requirements to ensure notice statements are accurately formulated, consent is given when necessary, that the person making the consent decision has the authority to do so, and that management of consent decisions is possible. The PCTF Notice and Consent Component specifies conformance criteria for processes that:

1. Formulate a statement about the collection, use, disclosure, and retention of personal information
2. Obtain a meaningful and informed consent decision based upon that statement from a person authorized to do so

The scope of the PCTF Notice and Consent Component and associated conformance criteria includes:

1. The collection, use, disclosure, and retention of personal information for the purposes of establishing and asserting a digital identity and related verified Subject-Specific Personal Information
2. Consent being obtained by a different organization than the one collecting, using or disclosing data – circumstances that could arise in a federated identity system
3. A single consent being obtained where multiple pieces of personal information are being collected, used or disclosed by multiple organizations, as part of a single transaction
4. Situations where the Subject may or may not have an explicit relationship with the information provider (e.g., where a background check is performed against a third-party source in accordance with relevant legislation)
5. Disclosure (or sharing) of data may follow either a "request" or "enquiry" mode

The scope of Notice and Consent Component does not include:

1. The subsequent use of personal information by the organizations in the delivery of their services. The handling of Subject-Specific Personal Information by a Requesting Organization is subject to relevant legislation, policy, and/or regulations and is not generally deemed to fall within the scope of the requirements of the Digital Identity Ecosystem once that data has been shared outside the Digital Identity Ecosystem. An exception to this is when a Disclosing Organization has specific requirements on the handling of personal information by its destination (the Requesting Organization). These requirements will thus form part of the digital identity ecosystem's governance and constitute "downstream" requirements with which any Requesting Organization receiving data from that Disclosing Organization must comply.
2. Use cases where another person acts on behalf of the Subject (e.g., power of attorney, a parent acting on behalf of a child). This version of the Notice and Consent Component only considers Subjects providing consent for the collection, usage, disclosure, and retention of personal information about themselves. Those use cases will be added in a future version.

3.1.9 Infrastructure: Technology and Operations

The PCTF Infrastructure: Technology and Operations component specifies conformance criteria that provide general requirements and guidelines regarding the trustworthiness of the IT infrastructure that enables implementation and delivery of the trusted processes defined in other PCTF components. The component's primary subject areas are the security and integrity of technical components. Within these areas of interest, the component's scope includes:

1. IT security (as a general consideration)
2. Preserving the confidentiality and integrity of supporting IT infrastructure
3. Oversight of data collection, validation, storage, and accessibility
4. Audit and logging.
5. Prevention of and response to IT events that compromise the trustworthiness of the digital identity ecosystem.
6. Formal policies and plans supporting the trustworthy management of technology and technology operations.

This scope of this PCTF component does not include:

1. The suitability of specific products to support a given trusted process
2. The suitability of specific standards, processes, or protocols that may be mandated by an individual Digital Identity Ecosystem
3. Mandating the use of a specific set of standard practices or frameworks to govern technology operations (e.g. ITIL, COBIT)

3.1.10 Privacy

The PCTF Privacy component specifies conformance criteria that define general requirements to ensure the ongoing integrity of the privacy processes, policies, and controls of organizations in a Digital Identity Ecosystem. The PCTF Privacy Component is concerned with the handling of personal data for digital identity purposes.

The Conformance Criteria of the PCTF Privacy component specify how the PIPEDA Fair Information Principles, defined by the Office of the Privacy Commissioner of Canada, apply to the handling of digital identity information. As such, the scope of this PCTF component is aligned with PIPEDA's 10 Fair Information Principles, which are:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure, and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

Privacy by design is one of DIACC's guiding principles for a Canadian Digital Identity Ecosystem, specifically "To, Implement, protect, and enhance privacy by design". Privacy considerations are integral to and should be taken into account at all stages of the development of a digital identity solution. For this reason, Conformance Criteria specified in the PCTF Privacy Component may be applicable to trusted processes and conformance criteria specified in other PCTF components – and are therefore regarded as encompassing all other components in a PCTF context.

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 to assess the trustworthiness of 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 regulations; participants in the Digital Identity Ecosystem are expected to meet the applicable legal and regulatory requirements in their jurisdictions.

In keeping with the guiding principles in section 2.5, which advocate 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 requirements they represent can be assessed. This allows participants 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*.

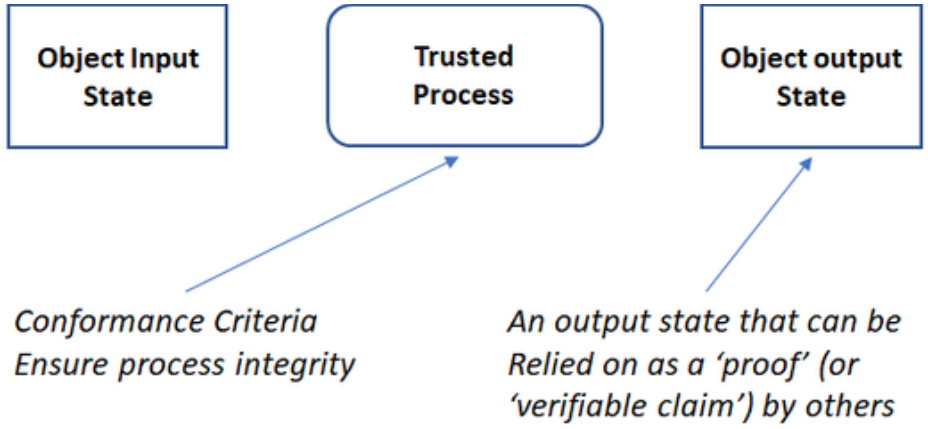

Figure 2. Trusted Process Model

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 not because of inherent natural protections but because 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 DIACC stakeholders to tailor baseline conformance criteria to specific requirements or applications. This could include, but is not limited to:

- requiring mandatory compliance with conformance criteria defined as optional in the baseline;
- 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** of **subjects**;
- When processing digital representations, participants perform one or more **roles** in the ecosystem;
- Each role consists of 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 an entity that can be uniquely identified with a context, is subject to legislation, policy, or regulations within that context, and which may have certain rights, duties, and obligations. In the context of the PCTF, entities that may hold or be in the process of obtaining a digital representation within the ecosystem are referred to as Subjects. 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** – A biological individual, human being who is alive or deceased. Examples of persons include residents of a jurisdiction (country, province, etc.), the customers of a business, and private individuals.
2. **Organizations** – An entity that consists of a person or organized body of people with a particular purpose, and whose existence is established by legal statute. Examples of organizations include businesses (including sole proprietorships, partnerships, and corporations), government agencies, co-operatives, and registered charities.
3. **Machines** – Software and hardware that can act as intelligent agents to conduct transactions independently (i.e., requires identity verification of the machine). Such machines that act on behalf of a person or an organization are typically 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, followed by those for *organizations*. 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, deletion. 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, or organizations (public, commercial, or non-profit) that agree to operate within the parameters of the PCTF. In the PCTF model, participants that perform key processes in the lifecycle of digital representations assume one or more roles that are defined as:

Function	Role	Description
Create and manage digital representations	Identity providers	A role that a participant performs to create, maintain and provide digital representations. Sometimes referred to as identity service providers or identity issuers. In some cases, the subject is the creator and manager of its own identity (e.g., in certain self-sovereign use cases).

	Credential providers	A role that a participant performs to create and manage credentials. Sometimes referred to as attribute providers.
	Authentication Service Provider	A role that a participant performs to create and manage authenticators. Sometimes referred to as credential service providers. These are not the same as PCTF Credential Providers. See section 5.1.3 for details.
Use digital representations	Relying parties	A role that an Organization or Person performs to consume digital representations created and managed by participants to conduct digital transactions with subjects.
	Subjects	A Person, Organization, or Machine that holds or is in the process of obtaining a digital representation in the digital identity ecosystem system regulated by the PCTF, and that can be subject to legislation, policy and regulations within a context The subject of a digital representation may assume explicit functions and/or responsibilities (e.g., a duty to safeguard the digital representation and prevent abuse). There may also be implicit functions performed by the subject in the context of the Digital Identity Ecosystem (e.g., functions associated with “motivation to recover” a digital representation that has been compromised or corrupted).
Enable digital identity systems	Infrastructure providers	A role that a participant performs to provide the physical and electronic infrastructure needed to enable digital interactions.
	Accredited Assessors	A role that a participant performs to conduct assessments of another participants' compliance with the PCTF, including PCTF conformance profiles.

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).

Those stakeholders unable to fully participate in the identity ecosystem (e.g., due to cost or delays in conformance assessment, which could present a burden to start-up companies) can reuse technology and processes put in place by the PCTF participants as part of efforts to more fully participate in some role or capacity. This gives the PCTF the potential to lower barriers-to-entry to the identity ecosystem.

4.3 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 (i.e., a person, organization, or machine) 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, addresses, former names, phone numbers, and 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** – Information or biometric characteristics under the control of an individual that is a specific instance of: something the Subject has, something the Subject knows, or something the Subject is or does. Examples of common authenticators are private signing keys, user passwords, or a person's face.

5.1.1 Identities

Digital identities are electronic representations that refer to distinct entities within the ecosystem; parties wishing to interact with each other. Identities consist 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.

5.1.1.1 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 subjects.	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 subjects 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

5.1.1.2 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. 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?”. Examples of credentials are:

- a simple construct that attests to a person’s age or a business’ registration status in a given province
- a complex construct that represent university transcripts, employment histories, or position within an organization

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 includes one or more identifiers and attribute values generated by the credential issuer. Depending on implementation details:

- identifiers may be pseudonymous; and
- it may be possible to cryptographically verify attribute values.

In the context of this document, a credential is not synonymous with a username and password or similar mechanism used to control access to a managed system. In the PCTF model overview 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;
- information stored in the credential is current and accurate; and
- credentials are appropriately destroyed at the end of their useful life-cycle.

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

- credential information can be disclosed as needed and according to specified conformance criteria;
- relying parties can verify disclosed information contained in a credential according to circumstances and implementation details (e.g., in its entirety, select pieces of data, or as a zero-knowledge proof); and
- relying parties can verify credential status (e.g., whether or not the credential has been revoked or otherwise rendered invalid).

5.1.2.1 Types of Credentials

The PCTF defines two 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. 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.
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.

5.1.2.2 Processes Typically Performed by Credential Providers

Process	Description
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.
Identity-credential binding	The process of associating credentials to an attributed actor.
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.
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

Information or biometric characteristics under the control of an individual that is a specific instance of: something the Subject has, something the Subject knows, or something the Subject is or does. Authenticators are used within the ecosystem to access restricted or protected systems (e.g., login protocol to 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".

Authentication Service 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, revocation, and destruction of authenticators).

5.1.3.1 Processes Typically Performed by Authentication Service 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 a pre-defined amount of time has passed, 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 the subject of a digital representation:

- **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.

- **Subject** – The entity represented by and to which data held in a digital representation pertains (e.g., the person whose age can be verified using a credential). In this context, the subject of the digital representation is typically a person who wishes to conduct a transaction, access a system, or interact with a relying party in some 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 subjects directly (i.e., in a peer-to-peer interaction without additional parties involved); and
- interactions may occur without direct involvement of the 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 (e.g., challenge-response questions) • Biological or behavioural confirmation (e.g., use of fingerprint) • Trusted referee confirmation (e.g., confirmation of identity based on information held by a government agency) • Physical possession confirmation (e.g., possession of a token or specific device)
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 the subjects of digital representations 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 another authorized person. 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 standards and guidelines 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 and policies for the lifecycle management of digital representation data, including oversight of data collection, validation, storage, accessibility, and destruction.
Technical standards	PCTF reference to relevant industry standards in support of specified functions, including interaction between Participants in the PCTF.

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. Typical risk categories include business processes, information management, information management, and stewardship of personal information.
Records management	Processes that support typical record-keeping activities for supported functions. This includes classification, retention schedules, preservation, and disposal.

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 Revision History

Version Number	Date of Issue	Authors	Description
0.01	2019-01-16	Gregory Natran	Initial draft recommendation for discussion
0.02	2019-02-04	Gregory Natran	Updated draft incorporating TFEC comments to date
0.03	2019-05-08	Gregory Natran	Updated draft incorporating feedback from the open review
1.0	2019-05-15	Gregory Natran	Draft Recommendation V1.0
1.1	2019-09-19	Gregory Natran	Updated draft incorporating latest public feedback
1.1.1	2019-10-18	PCTF Editing team	Update PCTF Components descriptions
1.1.2	2019-11-30	PCTF Editing team	Update definitions of terms to be consistent with the PCTF Glossary
1.1.3	2019-12-12	PCTF Editing Team	Updates per comments received during TFEC review that closed 6 December
1.1.4	2020-05-28	PCTF Editing Team	Updates based on revised scope statements "Verified Login" was changed to "Authentication" "Governance" was changed to "Assessment"
1.0	2020-07-02	PCTF Editing Team	Final Recommendation V1.0