PCTF Privacy Component Overview

Document Status: Final Recommendation V1.2

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

1. Introduction to the PCTF Privacy Component

This document provides an overview of the PCTF Privacy Component, a component of the Pan-Canadian Trust Framework (PCTF). For a general introduction to the PCTF, including contextual information and the PCTF goals and objectives, please see the PCTF Model Overview.

Each PCTF component is made up of two documents:

1. **Overview** – Introduces the subject matter of the component. The overview provides information essential to understanding the Conformance Criteria of the component. This includes definitions of key terms, concepts, and the processes or principles that are part of the component.
2. **Conformance profile** – Specifies the Conformance Criteria used to standardize and assess the integrity of the privacy processes, policies and controls of organizations in a Digital Identity Ecosystem.

This overview provides information related to and necessary for consistent interpretation of the PCTF Privacy Conformance Profile.

1.1. Purpose and Anticipated benefits

Privacy is a fundamental requirement of digital identity interactions. As such, all participants in the Pan-Canadian Trust Framework (PCTF) have a responsibility to follow privacy-respecting practices. Privacy-respecting practices rely on the principle that individuals know and understand the details and potential benefits, risk of harm and consequences associated with managing their personal information, and can take action based on that information.

The Privacy Component of the PCTF is concerned with the handling of personal data for digital identity purposes. The objective of the Privacy Component is to ensure the ongoing integrity of the privacy processes, policies and controls of organizations in a Digital Identity Ecosystem by means of standardized conformance criteria used for assessment and certification against the Pan-Canadian Trust Framework (PCTF). The Conformance Criteria for the Privacy Component specify tests that can be used to assess that an organization performing the role of Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Providers, or the Governing Body. The Conformance Criteria are designed to demonstrate that participants are handling digital identity information in alignment with the ten Principles defined in Schedule 1 of the Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) legislation. PIPEDA applies to organizations handling personal information in the course of commercial activities.

Note

The current set of conformance criteria are organized by the ten Principles for the Protection of Personal Information in Schedule 1 of PIPEDA[1]; however, they are intended to be broadly applied across private and public sector organizations. Future versions of this component may incorporate additional conformance criteria after review of other privacy guidance (e.g., Privacy by Design, PIPEDA modernization) and regulatory frameworks (e.g., federal and provincial privacy acts).

These conformance criteria do not replace existing regulations; organizations are expected to comply with relevant privacy legislation, policy and regulations in their jurisdiction.

Figure 1 provides a conceptual overview and logical organization of the Privacy Component.

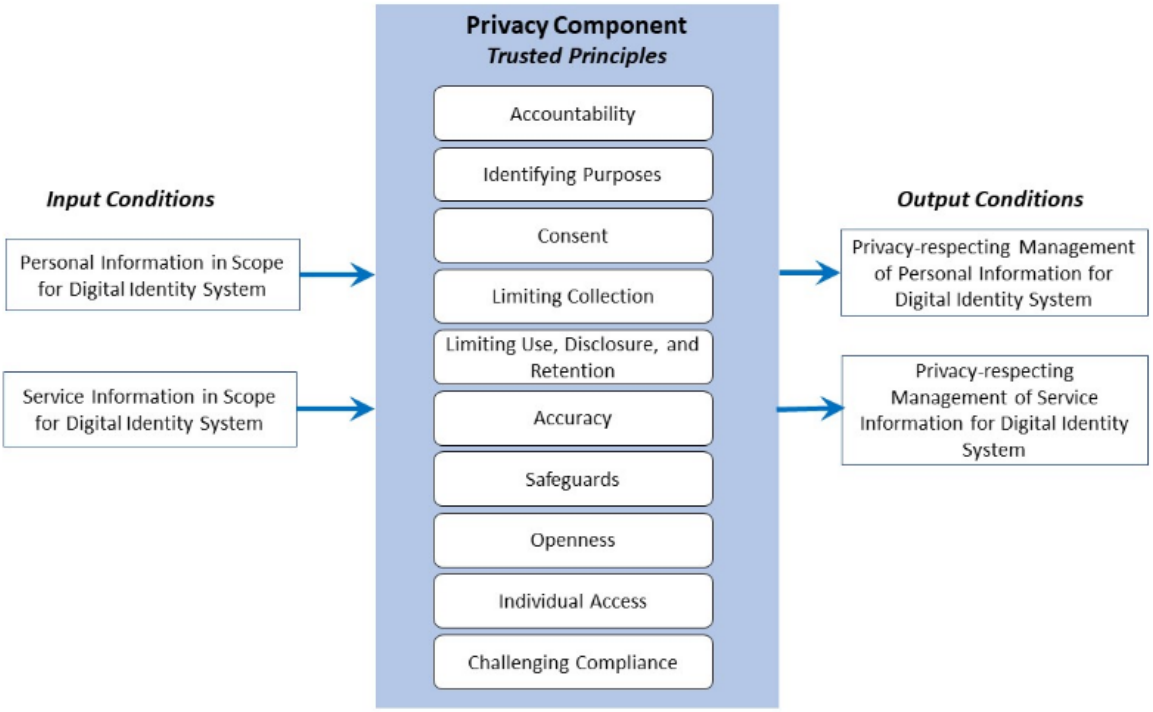

Figure 1. Privacy Component

The Privacy Component consists of elements that indicate the following:

- **Trusted Principles** – the set of principles that organizations (e.g., Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators) are expected to adhere to when handling subject-specific and service-specific personal information in a digital identity system. Each trusted principle is assessed using a set of conformance criteria associated with that principle.

- **Inputs** – input into trusted principles, for example, personal information requiring privacy management to proceed.
- **Outputs** – output resulting from trusted principles being applied, for example, privacy policies and controls applied to personal information.

1.2. Scope

Figure 2 illustrates the scope of the privacy component, which includes the functions performed by the Disclosing Organization, Requesting Organization, Notice and Consent Processor, as well as the Network Facilitator and Governing Body roles as described in the Roles section.

In the PCTF context, Personal Information (as defined in the Terms and Definitions section) will normally only be accessed by those performing roles that process digital identity information within the Digital Identity Ecosystem, and who will restrict access for those purposes. Participants that perform roles in the Digital Identity Ecosystem to enable, control and implement rules to facilitate the sharing of personal information, ideally (e.g., unless required by law)) should not be able to see, read, change, or be exposed to the information. The Notice and Consent Processor, which performs control functions, could be exposed to some personal information in (depending on how the Notice and Consent Processor is manifested), but this should be minimized (as per conformance criteria for limiting collection LIMC-9).

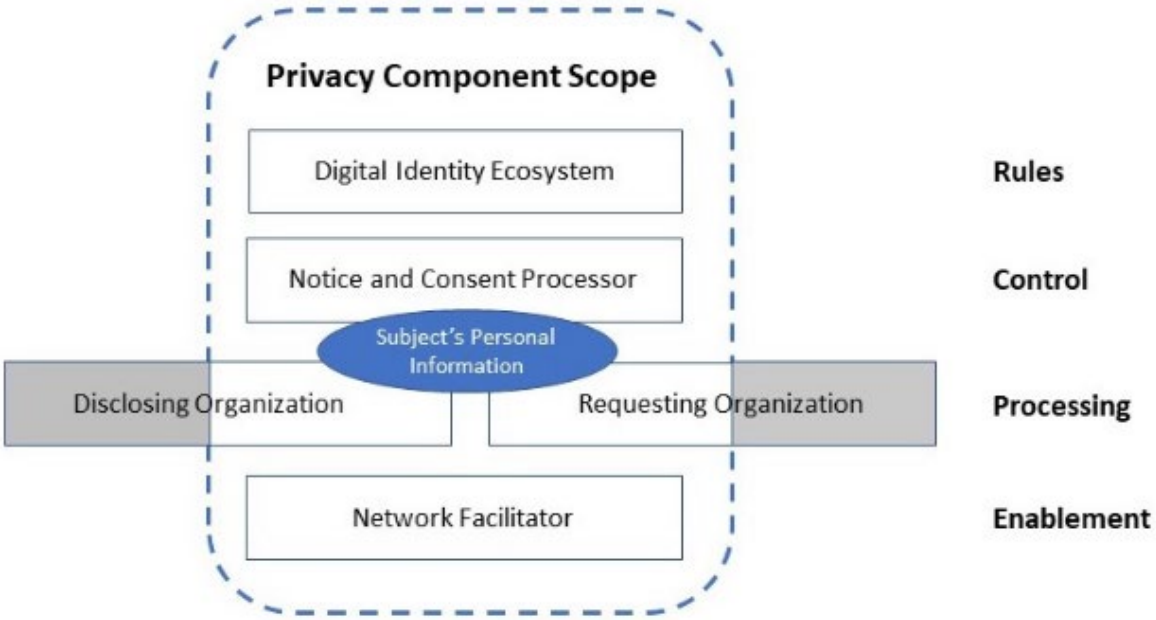

Figure 2. Privacy Component Scope and Roles

1.2.1. In-Scope

- Within the context of the PCTF, privacy requirements applicable to the roles within the Digital Identity Ecosystem. For an overview description of the PCTF model and its components, please refer to the PCTF Model Overview
- Requirements for the handling of Subject-Specific Personal Information and Service-Specific information associated with digital identity
- Privacy related policy and processes as they apply to delivery of assured digital identity

1.2.2. Out-of-Scope

- Fraud monitoring: The Privacy component does include conformance criteria that address breaches of privacy and fraud reporting for the roles specific to the Privacy component. Requirements for more general fraud monitoring, reporting, and actions to be taken within the Digital Identity Ecosystem warrant further consideration and development within the PCTF context. For reference, please consult the following criteria:
  - Baseline - BASE 6
  - For Governing Body - ACCO 2
  - For Notice and Consent Processor - CONS-21
- Specific related requirements addressed in other PCTF profiles (e.g. Delegated authority, Privacy and Security section of the Verified Organization Conformance Profile, requirement SOUR-01 in the Verified Person Conformance Profile)
- Baseline conformance criteria (See BASE in the Privacy Conformance Profile) do not address use cases where the Subject acts as the Disclosing Organization.
- Criteria variance dependent on LoA levels: The DIACC is currently working on the specifics of the LoA framework to be applied. While the work is mature enough to be reflected in some of the Profiles, it was felt that further detail was required in order to define any variances in criteria for the Privacy Component.

1.3. Relationship to the Pan-Canadian Trust Framework

The Pan-Canadian Trust Framework (PCTF) consists of a set of modular or functional components that can be independently assessed and certified for consideration as trusted components. Building on a Pan-Canadian approach, the PCTF enables the public and private sector to work collaboratively to safeguard digital identities by standardizing processes and practices across the Canadian Digital Identity Ecosystem.

Figure 3 is an illustration of the components of the Pan-Canadian Trust Framework. The Privacy Component encompasses all sub-components (i.e., Privacy related concerns are applicable to elements of all PCTF Profiles).

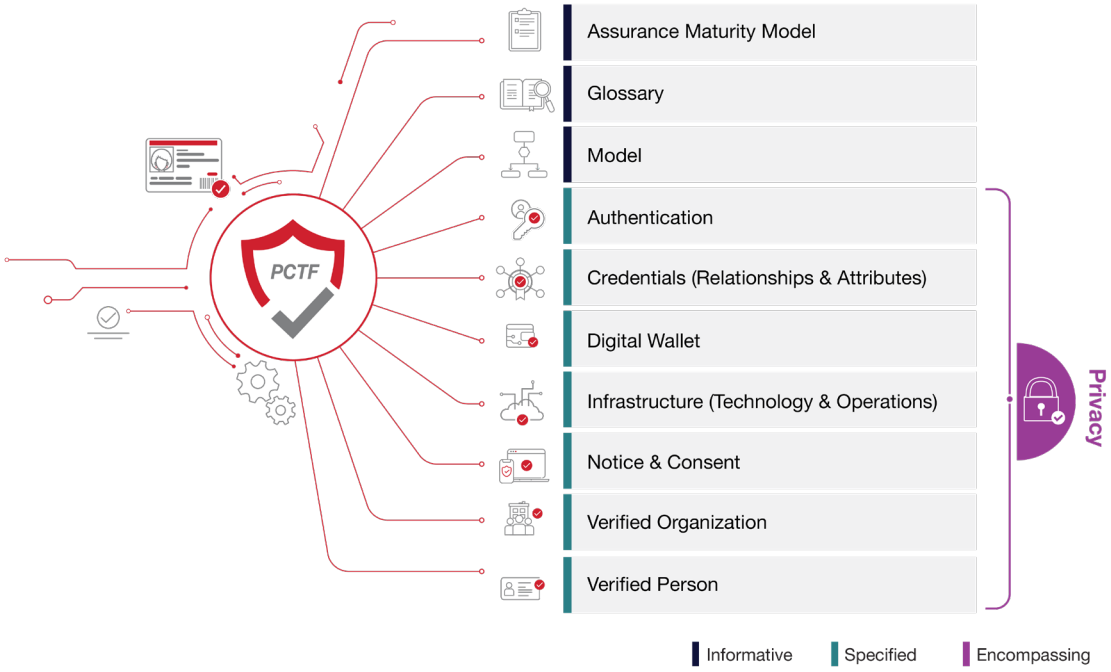

Figure 3. Components of the Pan-Canadian Trust Framework

PCTF conformance criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy and regulations in their jurisdiction.

2. Privacy Component Conventions

This section describes and defines key terms and concepts used in the PCTF Privacy Component. This information is provided to ensure consistent use and interpretation of terms appearing in this overview and the PCTF Privacy Conformance Profile.

2.1. Terms and Definitions

The Privacy component references the terms and definitions listed in the PCTF Glossary and specifically uses the following terms and definitions:

Subject

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. (Note: Delegated Authority is not addressed in this document).

User

A Person who is either the Subject or authorized to represent the Subject and intentionally accessing a digital service or digital program.

Notice

A statement that is formulated to describe the collection, use and disclosure of Personal Information and is presented to a User. May also be referred to as: consent form, or notice statement.

Consent

Permission, given from a User authorized to do so, to share Identity and/or Personal Information about a Subject as per the terms defined in a Notice. In the context of the PCTF, consent is equated to "Meaningful Consent" as described by the Office of the Privacy Commissioner of Canada and PIPEDA. May also be referred to as: consent decision.

Unless explicitly stated, consent in the Privacy component refers to express, or explicit, consent for sharing Personal Information, where the Subject must perform an action to provide consent. Implied consent, if applicable, will be identified as such in the criteria.

Personal Information

In general, Personal Information is defined as "Under PIPEDA, personal information includes any factual or subjective information, recorded or not, about an identifiable individual." For the purpose of this document, we define two types of Personal Information:

- **Service-Specific Information –** information collected or generated by the participants (Disclosing Organization, Requesting Organization, Notice and Consent Processor(s), or Network Facilitator) for purposes of operating and maintaining the service (e.g., service specific pseudonymous identifiers, transaction records, proofs of transactions including consent). In some cases, service-specific information may be shared, with subject's consent.
- **Subject-Specific Personal Information –** factual or subjective information about an identifiable Subject that is shared from a Disclosing Organization to a Requesting Organization (e.g., name, email address, phone number, mailing address, date of birth, account information).

Digital Identity Ecosystem

An interconnected system for the exchange and verification of digital identity information, involving public and private sector organizations (e.g., government,

commercial, non-profit, and other entities) who participate in, and comply with a common Trust Framework for the management and use of digital identities, and the Subjects of those digital identities. In the context of the Privacy component, the Digital Identity Ecosystem refers to a Canadian Digital Identity Ecosystem compliant with the PCTF. Participants in a Digital Identity Ecosystem may include Requesting Organization, Disclosing Organization, Notice and Consent Processor, Network Facilitator, and Governing Body as identified in the Scope section of this document.

3. Roles

The following roles in the Digital Identity Ecosystem are defined to cover the scope of the Privacy Component. Depending on the use case, separate organizations or persons may take on one or more roles.

- **Disclosing Organization –** A Role that an Organization or Person performs to hold Subject-Specific Personal Information, that the User consents to disclose to a Requesting Organization or that the Disclosing Organization can lawfully disclose under relevant legislation. In a digital identity context, this will often be an identity or attribute provider.
- **Governing Body –** A Role that a Participant performs to make sure that the standards, processes, and the associated requirements of the Digital Identity Ecosystem are implemented, which include conformance with government legislation, regulations and policy. They also enforce compliance by Digital Identity Ecosystem participants to agreed safeguards, guidance, best practices, rules and commercial arrangements.
- **Notice and Consent Processor –** A Role that a Participant performs to provide the notice to the User of the request for Personal Information (from the Requesting Organization), to obtain and record the consent and provides the User with the means to manage the consent going forward, including the withdrawal of consent.
- **Network Facilitator –** A Role that a Participant performs to connect parties together in a multi-party identity transaction. This organization is an active participant and adds value in the delivery of the digital identity service (e.g., not an internet service provider that passively provides internet connectivity). For example, a blockchain provider, or Software as a Service provider (SaaS) that facilitates the network.
- **Requesting Organization –** A Role that an Organization or Person performs to receive Personal Information that the User consents to disclose. In a digital identity context, this will often be a service provider or relying party.

These roles help to isolate the different functions and responsibilities with respect to privacy across the end-to-end processes for managing digital identities. They are not intended to imply any particular solution, architecture or implementation.

For example, in some cases, the notice may be presented and consent collected from an organization facilitating Personal Information exchange between the User, Disclosing Organization and Requesting Organization. In other cases, the notice may be presented and consent collected directly by either the Disclosing or Requesting Organization, in which case that organization would also be the Notice and Consent Processor.

4. Privacy Component Key Concepts

4.1. Personal Information

Privacy-respecting practices rely on the principle that individuals know and understand the details and potential benefits and consequences associated with managing their personal information, and can take action based on that information.

Personal information, as defined for the purposes of this Profile, includes Subject-Specific Personal Information and Service-Specific Information. This encompasses information that the user consents to disclose (e.g., name, email address, phone number, mailing address, date of birth, account information, etc.) as well as information required to operate and maintain the service (e.g., service specific pseudonymous identifiers, transaction records).

4.2. Changes of Personal Information at Source (a Disclosing Organization)

In the event of a change (including corrections) to Subject-Specific Personal Information, the Disclosing Organization is under no obligation within the Digital Identity Ecosystem to proactively notify any Requesting Organization that has previously received the Subject-Specific Personal Information, nor to flag that a change has been made, unless required by law. The onus is on a Requesting Organization to compare newly received data against previously received data for changes, and act on changes as relevant to their business processes.

4.3. Upstream and Downstream Handling of Personal Information

The handling of Personal Information by a Disclosing Organization is subject to relevant privacy legislation and regulations and is not generally deemed to fall within the scope of the requirements of the PCTF until that data is processed for the purpose of sharing via the Digital Identity Ecosystem. An exception to this is when a Requesting Organization has specific requirements on the handling of Personal Information by its source (the Disclosing Organization). These requirements will thus form part of the Digital Identity Ecosystem governance and constitute "upstream" requirements with

which any Disclosing Organization servicing that Requesting Organization must comply. Similarly, the handling of Personal Information by a Requesting Organization is subject to relevant privacy legislation and regulations and is not generally deemed to fall within the scope of the requirements of the PCTF once that data has been shared via 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 governance and constitute "downstream" requirements with which any Requesting Organization receiving data from that Disclosing Organization must comply.

4.4. Privacy by Design

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. Privacy-enhancing tools enable an individual to manage their information and what specified purpose(s) it is used for.

While the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), has recommended that PIPEDA be amended to include privacy by design principles [2], the current PIPEDA Fair Principles do not explicitly address privacy by design. As such, the Conformance Criteria of the PCTF Privacy Component do not include criteria to evaluate adherence to privacy by design.

5. Notes and Assumptions

More than one organization may be responsible for carrying out the Privacy trusted processes from end-to-end. The involvement of several organizations or persons may introduce complexity in the assessment and certification process, but the trust framework does not constrain different implementation approaches. Within the conformance profile three organizational roles are defined (requesting organization, disclosing organization and notice and consent processor). These help to isolate the different functions and responsibilities within the end-to-end process. They are not however intended to imply any particular solution, architecture or implementation.

Privacy-respecting practices rely on the principle that individuals know and understand the details and potential benefits and consequences associated with managing their personal information, and can take action based on that information. The specific requirements for this are addressed in the Notice and Consent PCTF Profile.

6. References

This section lists the external standards, guidelines, and other documents referenced in the PCTF Privacy component.

1. PIPEDA fair information principles, Office of the Privacy Commissioner of Canada, Revised: May 2019 and Schedule 1 of the Government of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96

2. Report of the Standing Committee on Access to Information, Privacy and Ethics, February 2018, Recommendation 14, p. 52

7. Revision History

Version Number	Date of Issue	Author(s)	Brief Description
0.01	2018-10-31	Consult Hyperion	Initial working draft
0.02	2018-11-22	DIACC	Terms for roles changed: • "Network" to "Network Provider' • "Eco-System" to "Governing Body"
0.03	2019-03-20	PCTF Editing Team	Updates for the discussion draft • Removed notice and consent content • Privacy principles • Describe the purpose of Privacy component
0.04	2019-05-09	PCTF Editing Team	Updated Privacy key component's descriptions
0.05	2019-06-26	PCTF Editing Team	Incorporated comments from discussion draft TFEC review
0.06	2019-10-31	Privacy Design and PCTF Editing Teams	Revised content based on discussion draft open review comments.
0.07	2019-11-22	PCTF Editing Team	Applied standard outline for PCTF Overview, which consolidates conceptual information in the Overview.

0.08	2019-12-11	PCTF Editing Team	Updated from Privacy design team meetings.
0.09	2020-01-02	PCTF Editing Team	Updated based on suggested editorial changes from open review.
0.10	2020-02-12	PCTF Editing Team	Updated based on several consultation sessions with TFEC expert team to review received TFEC comments
1.0	2020-02-12	PCTF Editing Team	Approved as Draft Recommendation V1.0
1.1	2021-10-29	PCTF Editor and Privacy Design Team	Updated in response to public comments
1.1	2021-11-10	PCTF Editor and Privacy Design Team	TFEC approves as a Candidate for Final Recommendation V1.1
1.2	2022-02-05	PCTF Editor and Privacy Design Team	Updated as per Privacy Design Team based on comments from public review
1.2	2022-03-02	PCTF Editor and Privacy Design Team	TFEC approves as a Candidate for Final Recommendation V1.2
1.2	2022-03-18	PCTF Editor and Privacy Design Team	DIACC sustaining members approved as Final Recommendation V1.2