Privacy Component Overview Discussion Draft Version 0.05

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

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

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

Notes:

- Governance of Privacy and other PCTF components are part of ongoing discussions. Comments from this review concerning governance will be referred to the PCTF Governance Design Team.
- Privacy-related requirements specific to notice and consent processes are detailed in the PCTF "Notice and Consent" component.

Table of Contents

1 Privacy Component Overview

Privacy is a fundamental requirement of digital identity interactions. As such, all components in the Pan-Canadian Trust Framework (PCTF) have a responsibility to follow privacy-respecting practices. Privacy-respecting practices rely on the principle that individuals are informed about the details and potential benefits and consequences associated with managing their personal 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 how the PIPEDA Fair Information Principles, defined by the Office of the Privacy Commissioner of Canada, are relevant/apply to the handling of digital identity data. (Note: These do not intend to replace existing regulations; organizations are expected to meet privacy regulations in their jurisdiction.)

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

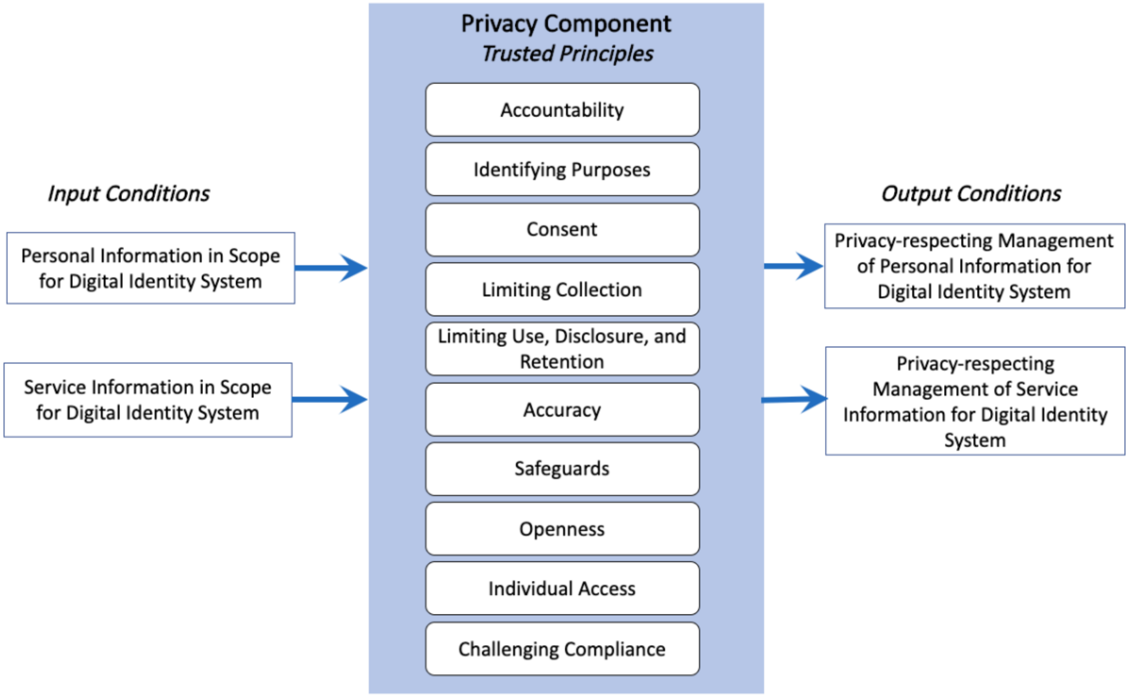

Privacy Component
Trusted Principles
Accountability
Identifying Purposes
Consent
Limiting Collection
Limiting Use, Disclosure, and Retention
Accuracy
Safeguards
Openness
Individual Access
Challenging Compliance
Input Conditions
Personal Information in Scope for Digital Identity System
Service Information in Scope for Digital Identity System
Output Conditions
Privacy-respecting Management of Personal Information for Digital Identity System
Privacy-respecting Management of Service Information for Digital Identity System

Figure 1. Privacy Component

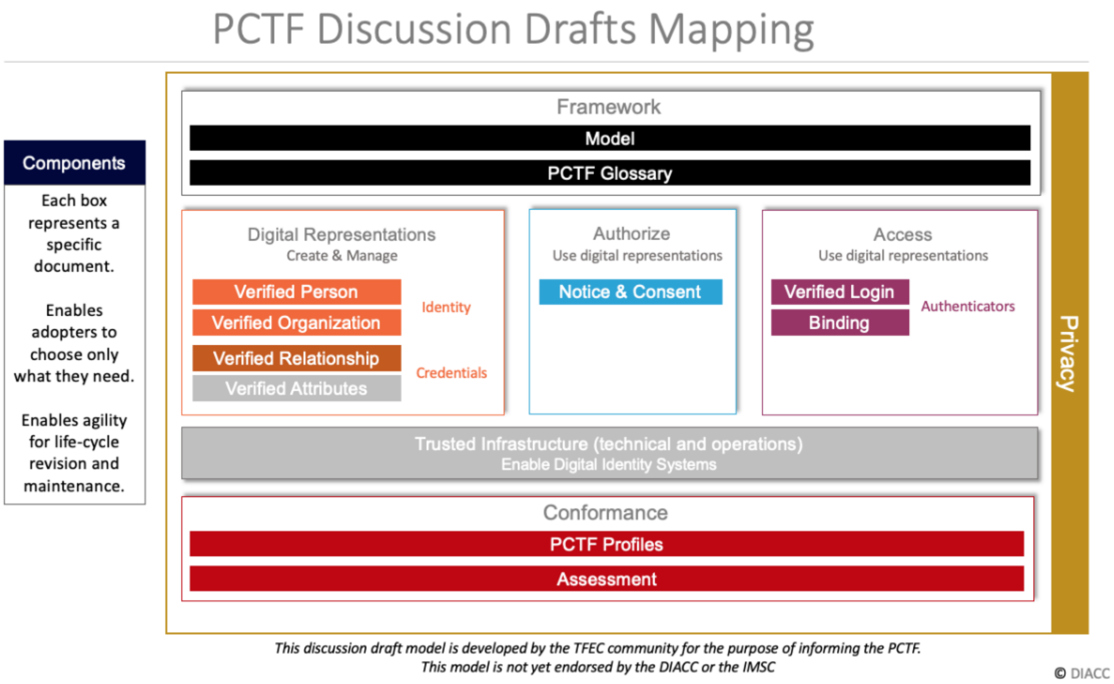
The Privacy Component consists of elements that indicate the following:

- **Trusted Principles** – the set of principles that organizations (e.g., Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Providers) are expected to adhere to when handling personal and service 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.

1.1 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 ecosystem.

Figure 2 is an illustration of the Pan-Canadian Trust Framework Model Visual Draft. The Privacy Component encompasses all sub-components.


PCTF Discussion Drafts Mapping
Components
Each box represents a specific document.
Enables adopters to choose only what they need.
Enables agility for life-cycle revision and maintenance.
Framework
Model
PCTF Glossary
Digital Representations
Create & Manage
Verified Person
Verified Organization
Identity
Verified Relationship
Verified Attributes
Credentials
Authorize
Use digital representations
Notice & Consent
Access
Use digital representations
Verified Login
Binding
Authenticators
Trusted Infrastructure (technical and operations)
Enable Digital Identity Systems
Conformance
PCTF Profiles
Assessment
Privacy
© DIACC

This discussion draft model is developed by the TFEC community for the purpose of informing the PCTF.
This model is not yet endorsed by the DIACC or the IMSC

Figure 2. Pan-Canadian Trust Framework Model Visual Draft

1.2 Scope

Figure 3 illustrates the scope of the privacy component and the function of different roles as described in the Privacy Conformance Profile. In the PCTF context, it is envisaged that personal information will normally be exposed only to the processing layer organizations. The other roles exist to facilitate the sharing of personal information but ideally should not be exposed to it.

The processing layer will also include the boundary to the outside world. There could potentially be some personal information in the control layer (depending on how the Notice and Consent Processor role is manifested in a particular digital identity system), but this should be minimized.

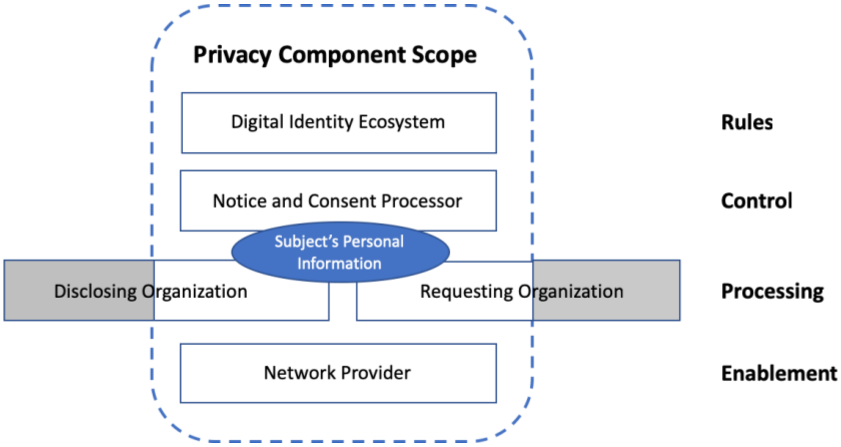


Figure 3. Privacy Component Scope and Roles

2 Privacy Component Key Concepts

2.1 Personal Information

Privacy-respecting practices rely on the principle that individuals are informed about the details and potential benefits and consequences associated with managing their personal information. Personal information includes information that the end-user consents to disclose (e.g., name, email address, phone number, mailing address, date of birth, account information, etc.) as well as information about operating and maintaining the service (e.g., service specific pseudonymous identifiers, transaction records)

2.2 Changes of Personal Information at Source (a Disclosing Organization)

The Disclosing Organization is under no obligation within the Digital Identity Ecosystem to proactively notify (e.g., push changes to) any Requesting Organization that has previously received the Subject's Personal Information, nor to flag that a change has been made. The onus would be 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.

2.3 Upstream and Downstream Handling of Personal Information

The handling of a Subject’s Personal Information by a Disclosing Organization is subject to relevant Privacy Regulations and is not generally deemed to fall within the scope of the requirements of the Digital Identity Ecosystem 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 that must be complied with by any Disclosing Organization servicing that Requesting Organization.

Similarly, the handling of a Subject’s Personal Information by a Requesting Organization is subject to relevant Privacy 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 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 that must be complied with by any Requesting Organization receiving data from that Disclosing Organization.

2.4 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[1], 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.

3 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 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.

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