PCTF Privacy Component Overview Draft Recommendation V1.0

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

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

Forthcoming PCTF releases will expand, clarify, and refine the content of this document.

The intended target audience for this draft are decision makers who may or may not be domain technology experts. When reviewing this draft, please consider the following and note that responses to these questions are non-binding and serve to improve the Pan-Canadian Trust Framework.

1. The PCTF Privacy component is a horizontal theme applicable to all other PCTF profiles. In this context, are the compliance criteria clear and comprehensive?
2. Do the documents strike the appropriate balance between elaborating privacy principles for digital identity aligned with PIPEDA, without being redundant with what PIPEDA says?
3. Could your organization identify any barriers to compliance (business, legal, or technical)?
4. Is the distinction between handling Subject-Specific Personal Information and Service-Specific Personal Information clear and complete?
5. Are Overview concepts clear and complete (e.g. key definitions, Digital Identity Ecosystem roles, Scope)?
6. The conformance criteria should be seen in the Pan-Canadian context of the PCTF and may not address specific additional requirements, reflected in policy or regulation, within a single jurisdiction or industry vertical. Within this context, are the conformance criteria clear and comprehensive?

NOTES:

- Criteria applicable to PCTF profiles addressing a specific component (e.g. Notice & Consent, Verified Login) are addressed in those profiles. Please refer to other component drafts if you are unsure if a particular topic is addressed.
- Privacy conformance criteria are meant to be technology and implementation method agnostic.

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 requirements that, when met, identify that an organization performing the role of Disclosing Organizations, Requesting Organizations, Notice of Consent Processors, Networks Providers, or the Governing Body is handling digital identity information in conformance 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: These do not replace existing regulations; organizations are expected to comply with relevant privacy legislation, policy and regulations in their jurisdiction.)

Future versions of this component may incorporate conformance criteria relevant to other privacy guidance (e.g., Privacy by Design, PIPEDA modernization) and regulatory frameworks (e.g., federal and provincial privacy acts).
Figure 1 provides a conceptual overview and logical organization of the Privacy Component.

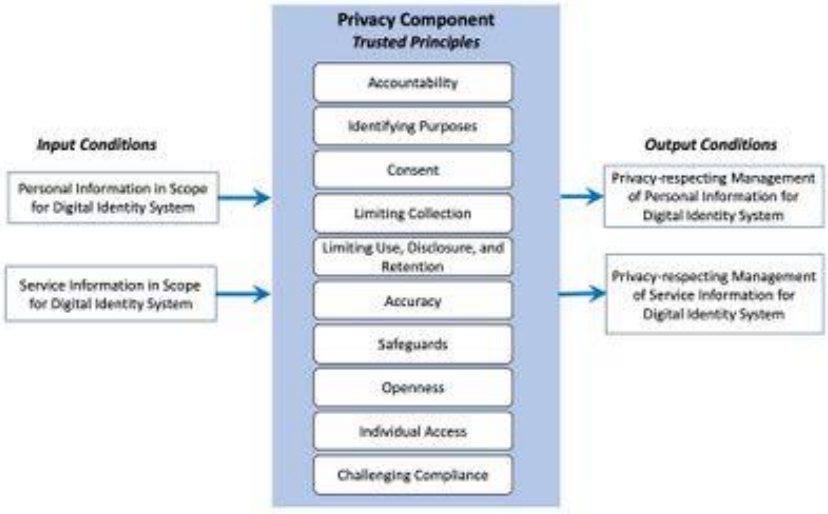

Figure 1. Privacy Component

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 3 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, Subject-Specific Personal Information will normally only be accessed by those performing roles that process digital identity information within the Digital Identity Ecosystem and will restrict access for those purposes. Participants that perform roles in the PCTF to enable, control and implement rules to facilitate the sharing of personal information ideally (e.g., unless required by law)) should not be exposed to it. 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).

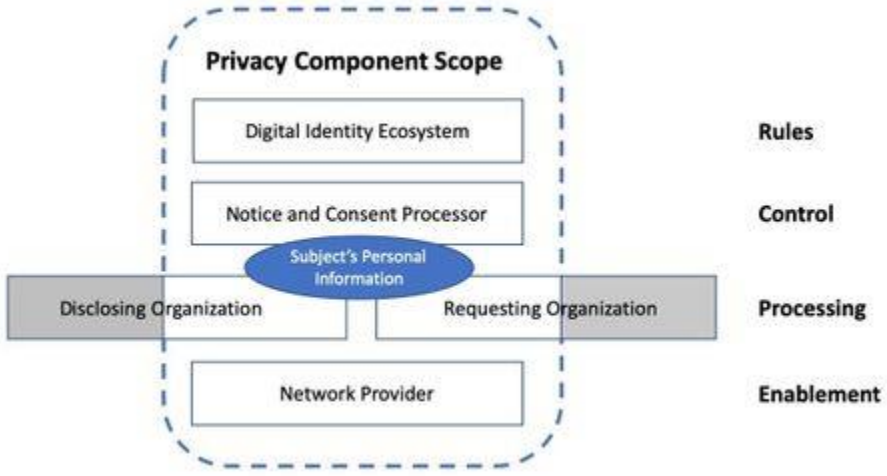

Figure 3. Privacy Component Scope and Roles

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
- Responsibility for the 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 (for all roles, see Baseline - BASE 6, for Governing Body see Accountability - ACCO 9, as well as Identifying Purpose IDENT-9, Consent CONS-23, and Limiting Collection LIMC-14). 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.
- Specific related requirements addressed in other PCTF profiles

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 2 is an illustration of the components of the draft Pan-Canadian Trust Framework. The Privacy Component encompasses all sub-components.

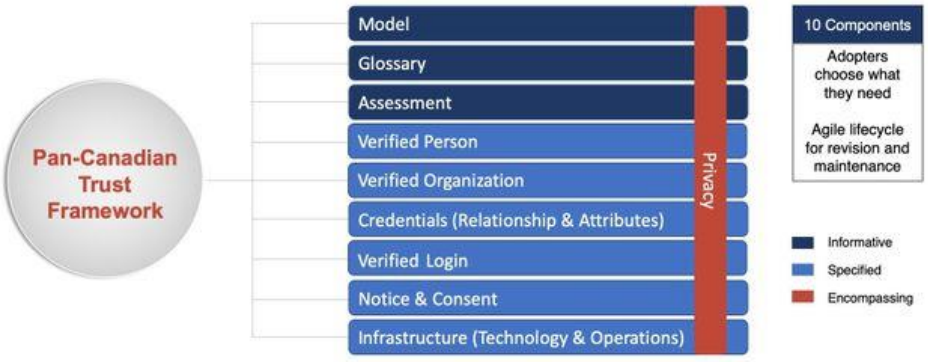

Figure 2. Components of the draft Pan-Canadian Trust Framework

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

2.1 Terms and Definitions

Notice
A statement that is formulated to describe the collection, use and disclosure of Personal Information and 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 –** information a Subject consents to share 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) that 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 the Canadian Digital Identity Ecosystem compliant with the PCTF.

2.2 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 may take on one or more roles.

- **Disclosing Organization –** the organization that currently holds the Subject-Specific Personal Information, that the Subject 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 –** the organization that oversees the trust framework and the associated requirements of the Digital Identity Ecosystem. This could involve providing governance as well as business, technical or commercial arrangements between the parties of the transaction.
- **Notice and Consent Processor –** the organization that provides the notice to the Subject of the request for Personal Information (from the Requesting Organization), obtains and records the consent and provides the Subject with the means to manage the consent going forward, including the withdrawal of consent.
- **Network Facilitator –** the organization that connects the 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 –** the organization that the Subject consents to disclose Personal Information to. In a digital identity context, this will often be a service provider or relying party.
- **Subject –** natural person to whom the Personal Information in question pertains. (Note: Delegated Authority is not addressed in this document).

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 Subject, 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.

3 Privacy Component Key Concepts

3.1 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 includes 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 about operating and maintaining the service (e.g., service specific pseudonymous identifiers, transaction records)

3.2 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[2] 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 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.

3.3 Upstream and Downstream Handling of Personal Information

The handling of a Subject-Specific 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 a Subject-Specific 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.

3.4 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.

4 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.

5 References

Footnotes

[1] Report of the Standing Committee on Access to Information, Privacy and Ethics, February 2018, Recommendation 14, p. 52
[2] This is not intended to absolve the Disclosing Organization of its legal/regulatory obligations.
PIPEDA in brief (Revised: May 2019)
Schedule 1 of the Government of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
ISO-27701