Notice and Consent Component Overview Discussion Draft Version 0.04

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.

Table of Contents

1. Notice and Consent Component Overview

The Notice and Consent Component defines a set of processes used to formulate a statement about the collection, use and disclosure of personal information, and to obtain a consent decision on that statement from a person authorized to do so. The Notice and Consent processes ensure that notice statements are accurately formulated according to defined requirements, that the person making the consent decision has the authority to do so, and that the management of that consent decision is possible.

The objective of the Notice and Consent Component is to ensure the ongoing integrity of the notice and consent processes by applying standardized conformance criteria for assessment and certification. A certified process is a Trusted Process that can be relied on by other participants of the Pan-Canadian Trust Framework.

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

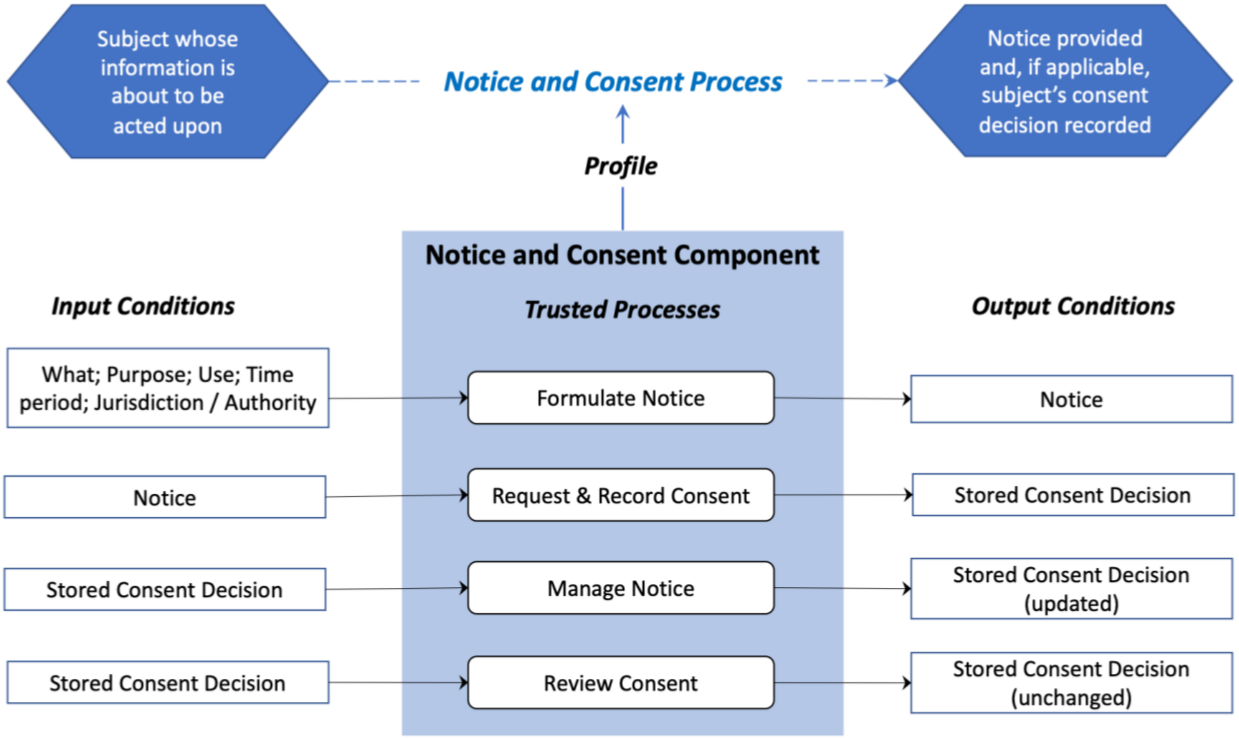
Subject whose information is about to be acted upon
Notice and Consent Process
Notice provided and, if applicable, subject's consent decision recorded
Profile
Notice and Consent Component
Input Conditions
Trusted Processes
Output Conditions
What; Purpose; Use; Time period; Jurisdiction / Authority
Formulate Notice
Notice
Notice
Request & Record Consent
Stored Consent Decision
Stored Consent Decision
Manage Notice
Stored Consent Decision (updated)
Stored Consent Decision
Review Consent
Stored Consent Decision (unchanged)

Figure 1. Notice and Consent Component

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. The Notice and Consent Component describes the "Authorize Information Use" block.

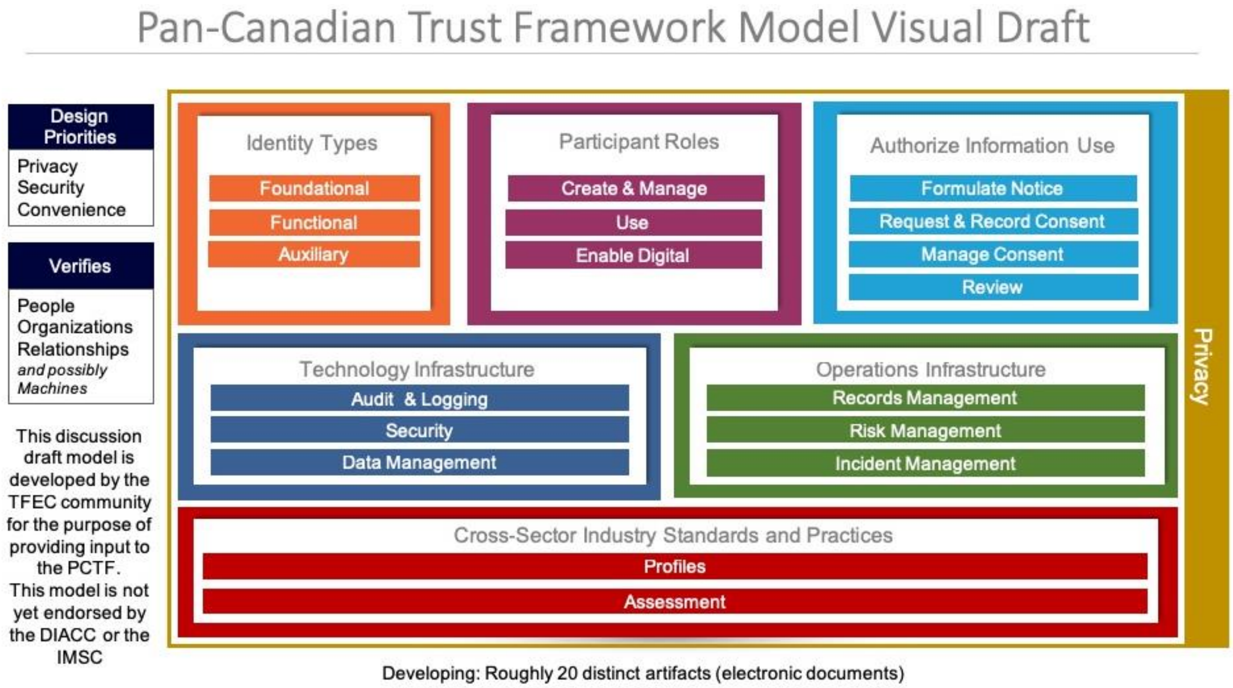
Pan-Canadian Trust Framework Model Visual Draft
Design Priorities
Privacy
Security
Convenience
Verifies
People
Organizations
Relationships
and possibly Machines
This discussion draft model is developed by the TFEC community for the purpose of providing input to the PCTF. This model is not yet endorsed by the DIACC or the IMSC
Identity Types
Foundational
Functional
Auxiliary
Participant Roles
Create & Manage
Use
Enable Digital
Authorize Information Use
Formulate Notice
Request & Record Consent
Manage Consent
Review
Technology Infrastructure
Audit & Logging
Security
Data Management
Operations Infrastructure
Records Management
Risk Management
Incident Management
Cross-Sector Industry Standards and Practices
Profiles
Assessment
Privacy
Developing: Roughly 20 distinct artifacts (electronic documents)

Figure 2. Pan-Canadian Trust Framework Model Visual Draft

2. Notice and Consent Trusted Elements

2.1 Trusted Processes and Conditions

A Trusted Process is a business or technical activity (or set of such activities) that transforms an input condition to an output condition. A condition is a particular state or circumstance that is relevant to a Trusted Process. It may be an input, output and/or dependency in relation to a Trusted Process. The conformance criteria specify what is required to transform an input condition into an output condition, for example, for a Request & Record Consent process to transform a "notice" input condition to a "stored consent decision" output condition. A trusted Notice and Consent business or technical process is assessed and certified according to conformance criteria stipulated by the Notice and Consent Conformance Profile and the Pan-Canadian Trust Framework.

2.2 Notice and Consent Trusted Processes

The Notice and Consent Component defines four Trusted Processes:

1. Formulate Notice
2. Request & Record Consent
3. Manage Consent
4. Review Consent

2.2.1 Formulate Notice

The Formulate Notice process generates a statement that describes what personal information is being collected, used or disclosed; what the purpose is for the collection, use or disclosure of the information; to whom the information will be disclosed; how the information will be handled and/or protected; the time period for which the notice is applicable; and under whose jurisdiction or authority the notice is applicable. This statement is presented to a person in the form of a notice statement.

2.2.2 Request & Record Consent

The Request Consent process ensures that the person who is being asked to provide consent has the authority to do so. This will typically involve identifying and authenticating the Subject using the Verified Person and Verified Login components of the PCTF. The Request Consent process presents the notice statement to the Subject and provides a capability for the Subject to accept or decline consent to the information in the notice, resulting in a consent decision. The subsequent Record Consent process makes a persistent record of the notice conditions and the Subject's consent decision. Examples of notice conditions that may be stored include information about the Subject, the date and time that the notice was presented, and the version of the notice presented. Examples of consent decision conditions that may be stored include the notice conditions, plus the consent decision made by the Subject, and, if applicable, the expiration date for the consent. Once the consent decision has been stored, the relevant parties to the consent decision are notified of the consent decision.

2.2.3 Manage Consent

The Manage Consent process manages the lifecycle of consent decisions and includes:

- renewing a consent decision involves the Subject establishing a revised consent decision from a previously stored consent decision based on a change in purposes or a period of time that has passed where there could be a change in circumstances since the previous consent;
- expiring a consent decision based on a set timeframe for its validity; or
- revoking a consent covers the Subject withdrawing the consent.

The Manage Consent process results in an updated consent decision that will need storing via the Request & Record Consent process.

2.2.4 Review Consent

The Review Consent process involves making the details of a stored consent decision visible to the Subject and authorized reviewers and follows proper privacy practices.

2.3 Notice and Consent Conditions

2.3.1 Input and Output Conditions

Table 1 specifies the input and output conditions for the Notice and Consent Component.

Condition	Description
What; Purpose; Use; Time Period; Jurisdiction/Authority	Specifics used to formulate a statement to which the Subject must consent in order to continue with the system process.
Notice	The presentation of the consent statement by the system to the Subject/recognized authority.
Consent Decision	The decision by the Subject to provide consent or decline consent.
Stored Consent Decision	The record of the notice and consent decision to a storage medium.

Table 1. Notice and Consent Component Conditions

2.3.2 Dependencies

Trusted Processes may need to rely on a condition that is the output of another Trusted Process. This is referred to as a dependency. Table 2 specifies the inputs, outputs, and dependencies between the Trusted Processes of the Notice and Consent Component.

Trusted Process	Input Condition	Process Dependency	Output Condition
Formulate Notice	What; Purpose; Use; Time period; Jurisdiction/ Authority	-	Notice
Request & Record Consent	Notice	Formulate Notice	Stored Consent Decision
Manage Consent	Stored Consent Decision	Request & Record Consent	Stored Consent Decision (updated)
Review Consent	Stored Consent Decision	Request & Record Consent	Stored Consent Decision (unchanged)

Table 2. Trusted Process Relationships

3. Levels of Assurance

Levels of assurance do not apply to the Notice and Consent Component as they do to the Verified Person or Verified Login Components. In those components, the levels of assurance indicate the robustness of the technology and processes employed to verify the person or login, respectively. In contrast, notice and consent requirements apply across all levels of assurance; there is no equivalent to “unverified” or “low assurance” for notice and consent. Even at low levels of assurance, consent should be obtained in broadly the same manner as at higher levels.

The notice and consent processes for sensitive data should require an appropriate level of assurance for the associated Verified Person and Verified Login.

4. Notes and Assumptions

More than one organization may be responsible for carrying out the Notice and Consent Trusted Processes from end-to-end.

For example, the Request Consent may be the responsibility of one organization, while the Record Consent may be the responsibility of a different organization. While the involvement of multiple organizations may introduce complexity in the assessment and certification process, the PCTF does not impose specific implementation approaches.

To help isolate the different functions and responsibilities within the end-to-end process, the Notice and Consent Conformance Profile defines three organizational roles (i.e., requesting organization, disclosing organization, and notice and consent processor). These delineations are not intended to imply any particular solution, architecture or implementation.