Notice and Consent Component Overview Draft Recommendation Version 1.0

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 is inclusive of decision makers who may or may not be domain technology experts.

Table of Contents

1. Notice and Consent Component Overview
   - 1.1. Relationship to the Pan-Canadian Trust Framework
   - 1.2. Scope
2. Notice and Consent Trusted Elements
   - 2.1. Trusted Processes and Conditions
   - 2.2. Notice and Consent Trusted Processes
     - 2.2.1. Formulate Notice
     - 2.2.2. Request Consent
     - 2.2.3. Record Consent
     - 2.2.4. Manage Consent
   - 2.3. Notice and Consent Conditions
     - 2.3.1. Input and Output Conditions
     - 2.3.2. Dependencies
3. Levels of Assurance
4. Notes

1 Notice and Consent Component Overview

The objective of the Notice and Consent Component is to ensure the on-going integrity of notice and consent processes by applying standardized conformance criteria for assessment and certification. A process that has been certified is a trusted process that can be relied on by other participants of the Pan-Canadian Trust Framework (PCTF). The PCTF conformance criteria are intended to complement existing privacy legislation and regulations; participants in the digital identity ecosystem are expected meet the applicable legislated requirements and regulations in their jurisdictions.

The Notice and Consent Component defines a set of processes used to:

- formulate a statement about the collection, use and disclosure of personal information
- obtain a meaningful and informed consent decision on that statement from a person authorized to do so.

The Notice and Consent processes ensure notice statements are accurately formulated according to conformance criteria, that the person making the consent decision has the authority to do so, and that management of that consent decision is possible.

Figure 1 provides a conceptual overview and logical organization of the Notice and Consent Component (given the scope defined for this component in Section 1.2).

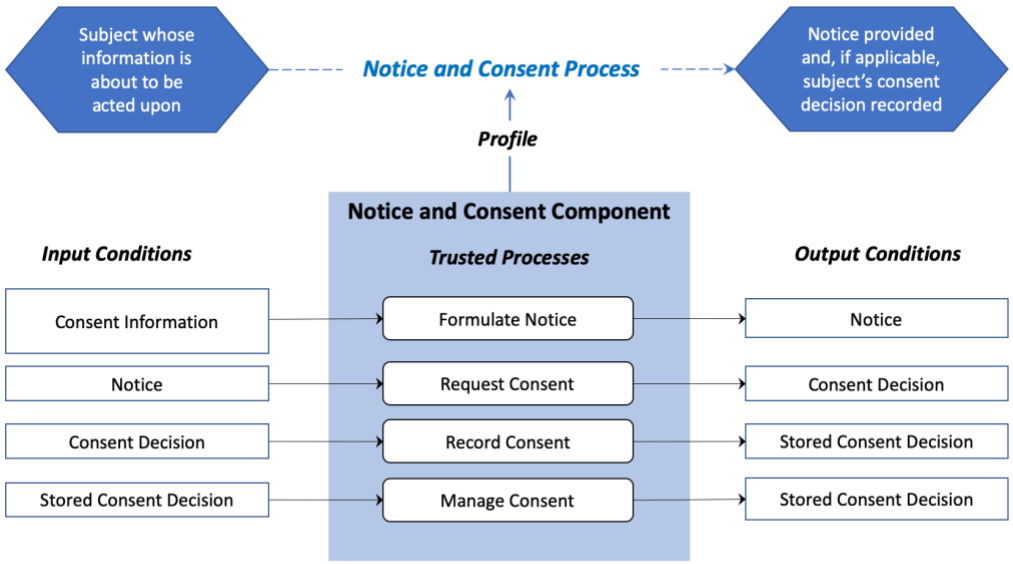


Figure 1. Notice and Consent Component

The Notice and Consent Component consists of elements that indicate:

- **Trusted Processes** – The set of processes that conform to conformance criteria (i.e., requirements) specified by the Pan-Canadian Trust Framework and which may be relied on (i.e., trusted) by others.
- **Conditions** – The particular states or circumstances relevant to making a consent decision.
- **Inputs** – Input into trusted processes, for example, a state requiring consent to proceed.
- **Outputs** – Output resulting from trusted processes, for example, a consent decision made by the subject.
- **Dependencies** – The relationship between trusted processes.
- **Profiles** – Additional criteria reflecting requirements or constraints that are relevant to a specific context (e.g., industry, public or private sector). Used to ensure consistency of implementation and facilitate the Pan-Canadian Trust Framework certification

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. Adopting 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 a logical overview of the Pan-Canadian Trust Framework. The Notice and Consent Component describes the "Authorize" block, which is part of the "use digital representations" functions. Note that the privacy requirements for the handling of personal information by the Notice and Consent processes (and all other PCTF components) within the digital identity ecosystem are defined in the PCTF Privacy Component.

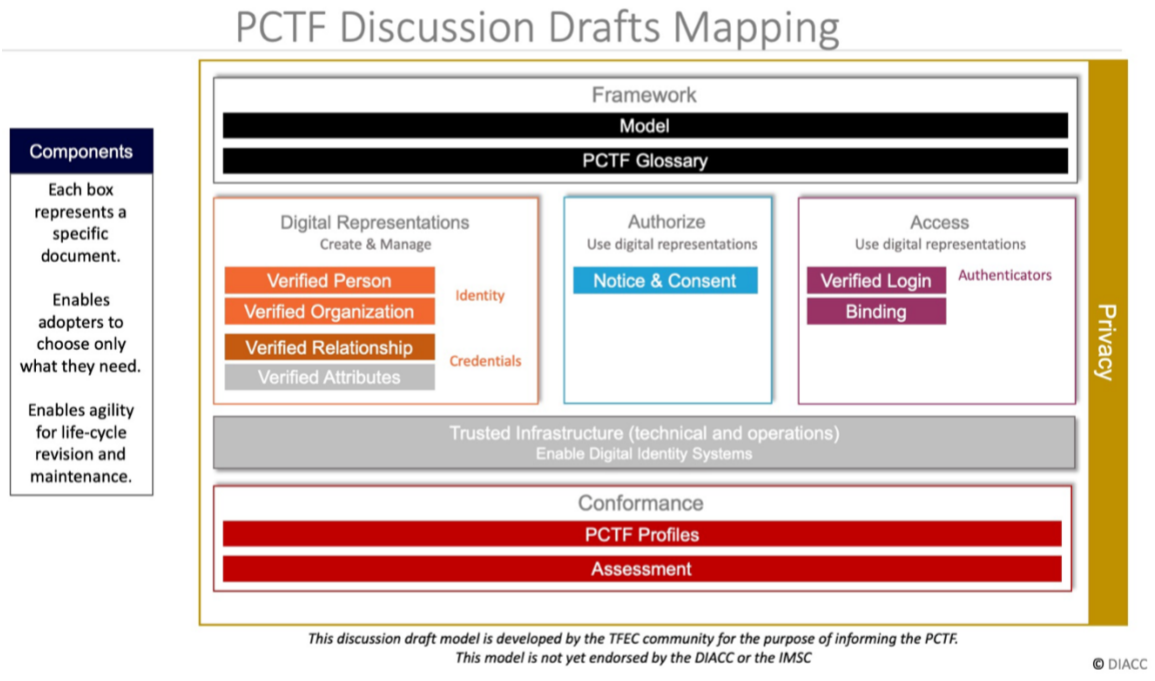


Figure 2. Pan-Canadian Trust Framework Model Visual Draft

1.2 Scope

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

- The collection, use and disclosure of personal information for the purposes of establishing and asserting a digital identity and related verified personal information.
    - Personal information in the context of the Notice and Consent Component refers to information (e.g., name, email address, phone number, mailing address, date of birth, account information) that a Subject consents to self-disclose or share from a Disclosing Organization to a Requesting Organization. This information is referred to as the Subject's Personal Information in the PCTF Privacy conformance criteria.
- Consent being obtained by a different organization than the one collecting, using or disclosing data – circumstances that could arise in a federated identity system.
- 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.
- 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); and
- Disclosure (or sharing) of data may follow either a "request" or "enquiry" mode
    - "Request" mode retrieves personal data from another party. Example: Asking "please provide attribute X that corresponds to Y?"
    - "Enquiry" mode has personal data corroborated by another party. Example: Asking "is the combination of X and Y valid?".

For digital identity systems, Notice and Consent is expected to be characterized as follows:

- Consent will normally be sought. While data protection laws allow for data to be collected without consent in certain circumstances (e.g., if disclosure is required to comply with a subpoena or legal requirement), these circumstances do not typically apply to digital identity solutions. Digital identity solutions are specifically concerned with providing visibility and control to Subjects over the collection, use, and disclosure of their personal information.
- Consent will always be "opt-in" (i.e., the Subject must perform an action to provide consent).
- Notice and consent must take place at the time of transaction that it applies to;
- Consent can be only for the transaction in progress (i.e., one time); or be given for a period of time (i.e., subscription services).
- Withdrawal of consent applies to future transactions where consent has been given for a period of time.
- Consent will always be explicit, and in language that is easily understood.
- Digital identity solutions will provide obvious and straightforward means for the Subject to manage consents, preferably in one place.
- The PCTF assumes that Notice and Consent will be digital and online whenever possible. However, guidance from the Office of the Privacy Commissioner of Canada includes, for example, ensuring that staff are appropriately trained to provide notice and obtain consent in in-person and non-automated situations. The PCTF is focused on digital identity, namely identity services that as far as possible are digital. Where it is necessary to employ manual processes, it is assumed the guidance from the Office of

the Privacy Commissioner of Canada or relevant legislation, regulation or policy as appropriate in the jurisdiction will be followed.

The scope of Notice and Consent Component does not include**:**

- The subsequent use of personal information by the organizations in the delivery of their services. 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.

  Similarly, 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.

- 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, and disclosure of personal information about themselves. These use cases will be added in a future version.

2 Notice and Consent Trusted Elements

2.1 Trusted Processes and Conditions

A process is a business or technical activity (or set of such activities) that transforms an input condition to an output condition; some transformations also depend on the output of another process. A business or technical process is designated as a trusted process when it is assessed and certified according to conformance criteria defined in the PCTF components and profiles.

In the Notice and Consent Component, for example, a Request Consent process transforms a "notice" input condition to a "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 Consent
3. Record Consent
4. Manage Consent

Note: It is not expected that all trusted processes and all associated conformance criteria will apply in all circumstances or use cases in the order presented above.

2.2.1 Formulate Notice

The Formulate Notice process generates a statement that describes the consent information that will be collected. The information required is based on applicable legal, policy and contractual requirements and could include, but is not limited to:

1. What personal information is being collected, used or disclosed;
2. What the purpose is for the collection, use or disclosure of the information;
3. To whom the information will be disclosed (organizations, individuals, or both depending on circumstances);
4. The source of the requested personal information, be it the Disclosing Organization or the Subject;
5. How the information will be handled and/or protected;
6. The time period for which the notice is applicable;
7. Under whose jurisdiction or authority the notice is applicable; and
8. Contact information for an authorized person who can answer the Subject's questions about the collection.

This statement is presented to a person in the form of a notice statement.

2.2.2 Request Consent

The Request Consent process presents the notice statement to a Subject and provides the capability for the Subject to accept (i.e., give) or decline (i.e., deny) consent based on the contents of the notice statement, resulting in a meaningful consent decision.

The Request Consent process must ensure that the Subject who is being asked to provide consent has the authority to do so. The Request Consent process will typically rely on trusted processes defined in other PCTF components (e.g., Verified Login, Verified Person, Verified Relationship) to authenticate the Subject, confirm Subject identity, and confirm Subject authority to make a consent decision. In this case, "authority to consent" is not always synonymous with "authority to collect"; a distinct authority (separate from consent) may be required to legally collect, use, or disclose information.

2.2.3 Record Consent

The Record Consent process makes a record of the notice conditions and the Subject's consent decision. This record is persistent and may be retained for historical reference even if the Subject subsequently revokes consent. 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 information that may be stored include the notice conditions along with the decision made by the Subject, date and time of consent and, if applicable, the expiration date for the consent.

Storage of notice conditions and consent decision information must comply with the legislation of the jurisdiction where the Record Consent is being applied. Once the consent decision has been stored, the relevant parties to the consent decision are notified of the consent decision.

2.2.4 Manage Consent

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

- Reviewing consent, which makes the details of a stored consent decision visible to the Subject and reviewers, and follows proper and applicable privacy practices.
- Renewing a consent decision, where the Subject establishes a revised consent decision from a previously stored consent decision based on a change in purpose 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.
- Revoking a consent, which includes the Subject actively withdrawing consent and situations where revocation results from other events (e.g., consent is found to be illegitimate).

The Manage Consent process results in an updated consent decision that can be stored via the Record Consent process.

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.

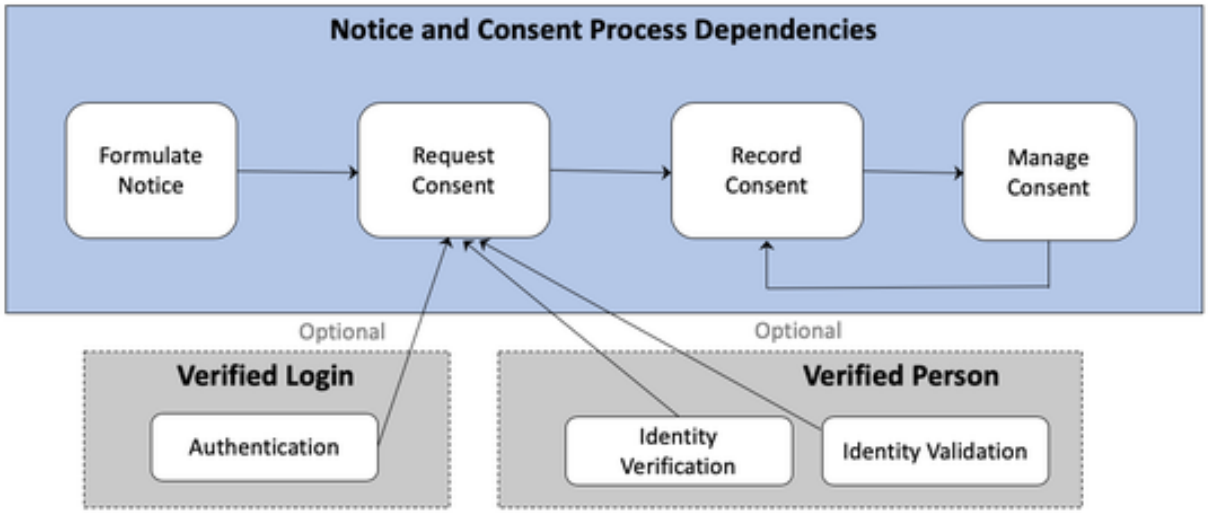
	Condition	Description
235-b	Consent Information	Information used to formulate a statement that is presented to a Subject to obtain the consent necessary to continue with the system process. Consent information includes: What data is required; Purpose; For Whom; How its protected; Time Period; Jurisdiction/Authority
235-c	Notice	The presentation of the required consent information in a statement by the system to the Subject or recognized authority.

235-d	Consent Decision	The presentation of the required consent information in a statement by the system to the Subject or recognized authority.
235-e	Stored Consent Decision	The record of the notice conditions and consent decision to a storage medium.

236 **Table 1. Notice and Consent Component Conditions**

237 2.3.2 Dependencies

238 Trusted processes may need to depend on a condition that is the output of another
239 trusted process. Figure 3 illustrates the dependencies between the trusted processes of
240 the Notice and Consent Component, and trusted processes in other PCTF components.



241

242 **Figure 3. Trusted Process Dependencies**

243 3 Levels of Assurance

244 Levels of assurance are used in certain contexts, such as those described in the PCTF Verified
245 Login Component or the PCTF Verified Person Component, to indicate the robustness of the
246 technology and processes employed to verify the login or the identity of an individual. Notice
247 and consent requirements apply across all levels of assurance; there is no equivalent to
248 “unverified” or “low assurance” for notice and consent trusted processes.

249 Consent should be obtained in broadly the same manner at low levels of assurance as it is at
250 higher levels of assurance.

251

4 Notes

- 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, and 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, in the Roles section of the Conformance Profile, three organizational roles (Disclosing Organization, Requesting Organization, and Notice and Consent Processor). These delineations do not imply any particular solution, architecture or implementation.

- Notice and Consent may be required multiple times in a single digital identity flow. For example, a Subject may consent to a network provider (acting as a Requesting Organization), to share certain information and, as part of a collaborative service arrangement, later consent during the same flow to another Requesting Organization using additional information not available from the network provider to support downstream business processes.