PCTF Notice & Consent Component Overview

Document Status: Final Recommendation V1.0

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.

This document is provided "AS IS," and no DIACC Participant makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third-party intellectual property rights, and fitness for a particular purpose. Those who are seeking further information regarding DIACC governance are invited to review the DIACC Controlling Policies.

Table of Contents

1 Introduction to the Notice and Consent Component

This document provides an overview of the PCTF Notice and Consent 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. It provides information essential to understanding the conformance criteria of the component. This includes definitions of key terms, concepts, and the Trusted processes that are part of the component.
2. **Conformance profile** – Specifies the Conformance Criteria used to standardize and assess the integrity of the Trusted Processes that are part of the component.

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

1.1 Purpose and Anticipated Benefits

The objective of the Notice and Consent Component is to ensure the on-going integrity of both the notice and consent processes by applying standardized conformance criteria for assessment and certification. A process that has been so 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 to comply with relevant privacy legislation and regulations in their jurisdictions.

Note

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.

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

- Formulate a statement about the collection, use, disclosure, and retention of personal information.
- Obtain a meaningful and informed consent decision based upon that statement from a person authorized to do so.

The notice, and the consent, processes ensure notices are accurately formulated according to conformance criteria, that the person making the consent decision has the authority to do so, that the consent is valid (i.e., freely given, specific, informed and unambiguous), 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 below).

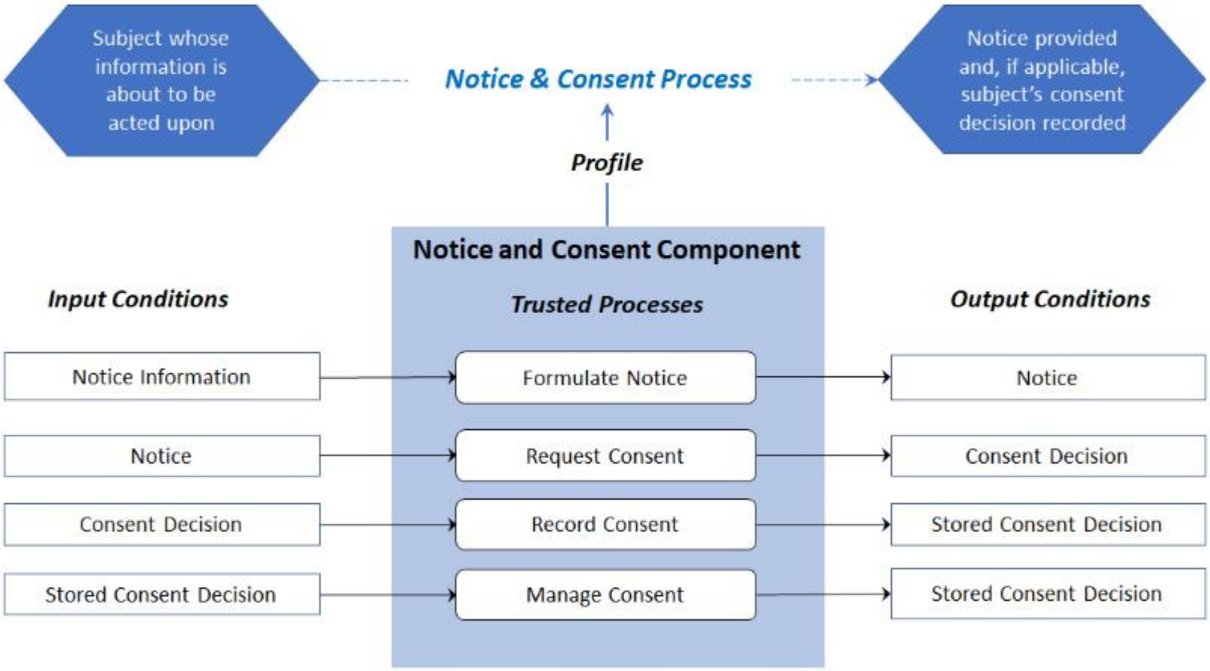

Figure 1. Notice and Consent Component

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

1.2 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 an illustration of the components of the Pan-Canadian Trust Framework. The Notice and Consent Component describes the processes and requirements to collect valid consent, which is integral but more specific than the general privacy requirements across the PCTF. 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.

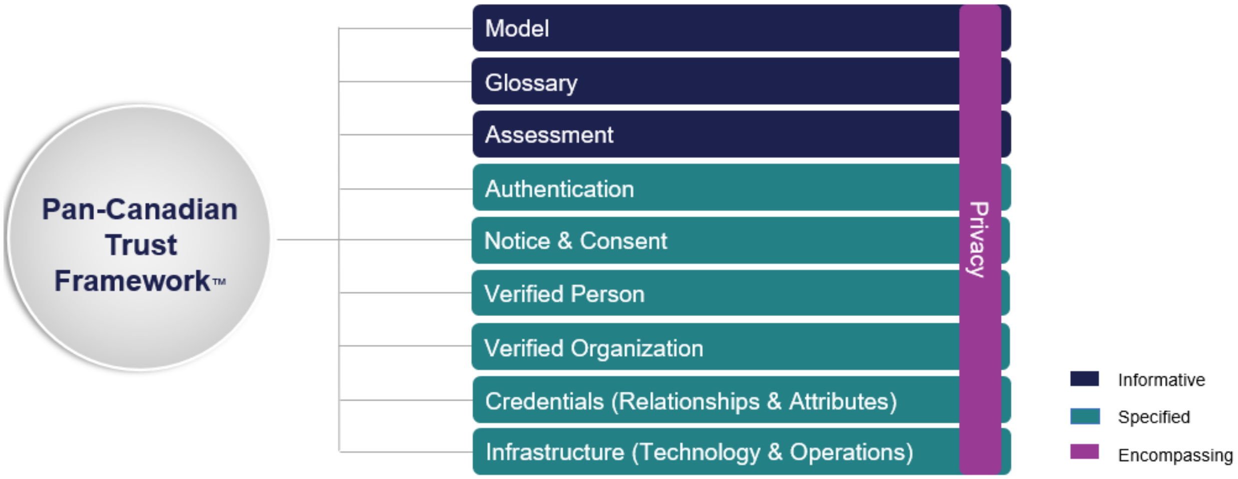

Figure 2. Pan-Canadian Trust Framework Model Visual Draft

1.3 Scope

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

- The collection, use, disclosure, and retention of personal information for the purposes of establishing and asserting a digital identity and related verified Subject-Specific Personal Information
- 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 in accordance with relevant legislation); 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 actively be sought. In cases where legislation or regulation does not require consent, notice should still be provided unless legislation, regulation, or policy prohibit it, or circumstances justify (e.g., collection or disclosure of data for an ongoing criminal investigation). 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). Digital identity solutions are specifically concerned with providing visibility and control to Subjects over the collection, use, and disclosure of their personal information.
- Express consent will always be required. That is, the Subject should always perform a deliberate action to provide consent for collection and/or disclosure of some, or all, of the information requested by the Notice and Consent Provider except in cases where legislation or regulation either prohibits, or does not require, consent.
- Both notice, and consent, should take place at the time of transaction that it applies to;
- Consent can either be given only for the transaction in progress (i.e., one time); or may be given for a period of time (i.e., subscription services).
- Previously granted consent may be revoked by the Subject at any time.
- Consent will always be explicit, and in plain language
- Digital identity solutions will provide obvious and straightforward means for the Subject to manage consents, preferably in one place.
- The PCTF assumes that both 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 in the appropriate jurisdiction will be followed. Additional guidance for obtaining meaningful consent in those cases can be found in the "Guidelines for obtaining meaningful consent" page of the Office of the Privacy Commissioner of Canada web site (https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/). Additional guidelines for training and accountability those cases can be found in the "Getting Accountability Right with a Privacy Management Program" area of the site (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/).

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 Subject-Specific Personal Information by a Requesting Organization is subject to relevant legislation, policy, and/or 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 outside 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's governance and constitute "downstream" requirements with which any Requesting Organization receiving data from that Disclosing Organization must comply.

Similarly, the handling of 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 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 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's governance and constitute "downstream" requirements that must be complied with by any Requesting Organization receiving data from that Disclosing Organization. For example, a healthcare agency that is a Disclosing Organization and has obligations that must be conveyed to a healthcare provider, which is a Requesting Organization (e.g., this identity can *only* be used for billing our agency), shall convey those obligations when the digital identity information is being exchanged.

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

1.4 Data Protection Laws and Notice and Consent

Digital identity is, by definition, concerned with providing entities with the digital means to collect, use and disclose verified personal information. Digital identity systems must, therefore, comply with data protection legislation, which includes requirements for notice and consent. The Notice and Consent Conformance Profile does not repeat legislative requirements, but shows how these requirements apply within the context of the PCTF.

Multiple data protection laws cover the operations of organizations when handling personal information. At a federal level, the Privacy Act and Personal Information Protection and Electronic Documents Act (PIPEDA) apply to federal government and commercial organizations respectively. Each province and territory has its own laws that apply to the handling of personal information by provincial and territorial public bodies. As well, several provincial statutes have been deemed "substantially similar" to PIPEDA and apply to how private sector organizations must handle personal information in those provinces.

Given these considerations, PIPEDA Schedule 1- Principle 3 (Consent), along with guidance from the Office of the Privacy Commissioner of Canada, provide a framework that can be applied to a range of organizations and use cases and is used as the basis for the PCTF Notice and Consent Component. If conflicts arise between the Notice and Consent Component and any data protection law applicable to an organization, then the applicable law takes precedence. 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).

2 Conventions

2.1 Terms and Definitions

For purposes of the Notice and Consent component, terms and definitions listed in the PCTF Glossary, as well as the following terms and definitions apply.

Subject

In the context of the Notice and Consent component, Subject always refers to a Person. Also, note that Delegated Authority, where a person is acting on behalf of a Subject is not addressed in this version.

Notice

A statement that is formulated to describe the collection, use, disclosure, and retention of Personal Information and inform a User. Notice requirements for each jurisdiction's legislation must be adhered to. May also be referred to as: **consent form**; **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. Consent requirements for each jurisdiction's legislation must be adhered to. May also be referred to as: **consent decision**.

In the context of the PCTF, express consent will always be required (i.e., the Subject must perform an action to provide consent); also referred to as express or explicit consent.

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 the PCTF Privacy, 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).

The Notice and Consent conformance criteria only consider Subject-Specific Personal Information, which is referred to as Personal 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 Abbreviations

No abbreviations.

2.3 Roles

The following roles are defined to cover the scope of the Notice and Consent conformance criteria. Depending on the use case, different organizations may take on one or more roles.

- **Disclosing Organization –** The organization that currently holds the personal information that the Subject consents to disclose to a Requesting Organization. In a digital identity context, this will often be an identity or attribute provider. Personal information verified by a Disclosing Organization and represented on a Subject's device is considered to be part of the Disclosing Organization.
- **Requesting Organization –** The organization to which the Subject consents to disclose personal information. In a digital identity context, this will often be a service provider or relying party.
- **Notice and Consent Processor –** The organization that provides the notice to the Subject of the request for personal information (from the Requesting Organization), unless not required or permitted due to legislation or regulation, obtains and records the consent and provides the Subject with the means to manage the consent going forward, including the withdrawal of consent.
- **Authorized Reviewer –** Participants impacted by a notice statement and/or consent request or approval (i.e., Disclosing Organization, Requesting Organization, and others described in this section), as well as regulatory bodies or oversight committees requiring access to a record of notice or consent for audit.

These roles help to isolate the different functions and responsibilities that participants may perform in end-to-end notice and consent processes. They do not imply any particular solution, architecture or implementation. For example, in some cases, the notice may be presented, and consent collected, from a network operator (acting as Notice and Consent Processor) facilitating personal information exchange between a patient (the Subject), a medical lab (Disclosing Organization) and a hospital (Requesting Organization). In other cases, the notice may be presented, and consent collected, directly by either the Disclosing Organization or Requesting Organization, in which case that organization would also be the Notice and Consent Processor.

2.4 Levels of Assurance

Levels of assurance are used in certain contexts, such as those described in the PCTF Authentication Component or the PCTF Verified Person Component, to indicate the robustness of the processes employed to verify the login or the identity of an individual. Notice and consent requirements apply across all levels of assurance; there is no equivalent to "unverified" or "low assurance" for notice and consent trusted processes.
Consent should be obtained in broadly the same manner at low levels of assurance as it is at higher levels of assurance. As such, the Notice and Consent Component conformance criteria reflect the following:

- Disclosure of sensitive data (e.g., health-related attributes) should only be done with an appropriate level of assurance for the associated Verified Person and Authentication (see CONS 3) and in accordance with relevant legislation.
- Consent can be recorded in different ways with different levels of robustness. For example, a flag in a database could indicate the user checked a box. For the consent given, a digital signature may provide a greater level of non-repudiation than clicking a checkbox. This version of the Notice and Consent Conformance Profile does not differentiate between such approaches but does require a minimum level of robustness of the consent process to satisfy regulatory requirements (see RECO 1).

3 Trusted Processes

3.1 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.

3.2 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, nor that they will occur in the order presented above.

3.2.1 Formulate Notice

The Formulate Notice process generates a statement that describes the 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, disclosure, or retention 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;
8. Contact information for an authorized person who can answer the Subject's questions about the collection; and
9. Additional information required by relevant legislation, policy, and regulations in the relevant jurisdiction.

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

3.2.2 Request Consent

The Request Consent process presents the Notice 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, resulting in a meaningful consent decision.

The Request Consent process is intended to 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., Authentication, Verified Person, Verified Relationship) to authenticate the Subject, confirm Subject identity, and confirm Subject authority to make a consent decision.

3.2.3 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. In some cases, retention may be subject to legislation or regulations. Examples of notice conditions that may be stored include information about the Subject, the recognized authority that provided consent (if applicable), 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, the date and time of consent and, if applicable, the expiration date for the consent. Though records of consent should store information about the *type* of data a Subject consented to share, they should not contain the Subject's data. (e.g., such a record might indicate that a Subject consented their address *be used* but would not contain their actual address.) While consent may be revoked or changed as previously mentioned, records of consent should not be altered.

Storage and/or retention of notice conditions and consent decision information must comply with the legislation and regulations of the jurisdiction(s) 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. Records of consent can, and should, be destroyed when no longer needed, provided that is compliant with relevant legislation and regulations.

3.2.4 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 authorized reviewers, follows proper and applicable privacy practices, and respects relevant legislation, regulation, and policy. Note: Authorized reviewers are participants impacted by the consent (i.e., Disclosing Organization, Requesting Organization) as well as regulatory bodies or oversight committees for audit.
- Renewing a consent decision, where the Subject or recognized authority 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 fraudulent).

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

3.3 Notice and Consent Conditions

3.3.1 Input and Output Conditions

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

Condition	Description
Notice Information	Information used to formulate a statement that is presented to a Subject to formulate an appropriate Notice and, if applicable, to obtain the consent necessary to continue with the service process. The information required is based on applicable legal, policy and contractual requirements.
Notice	The presentation of a statement containing the Notice Information to the Subject.

Consent Decision	The decision by the Subject to provide consent or decline consent.
Stored Consent Decision	The record of the notice conditions and consent decision to a storage medium.

Table 1. Notice and Consent Component Conditions

3.3.2 Dependencies

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

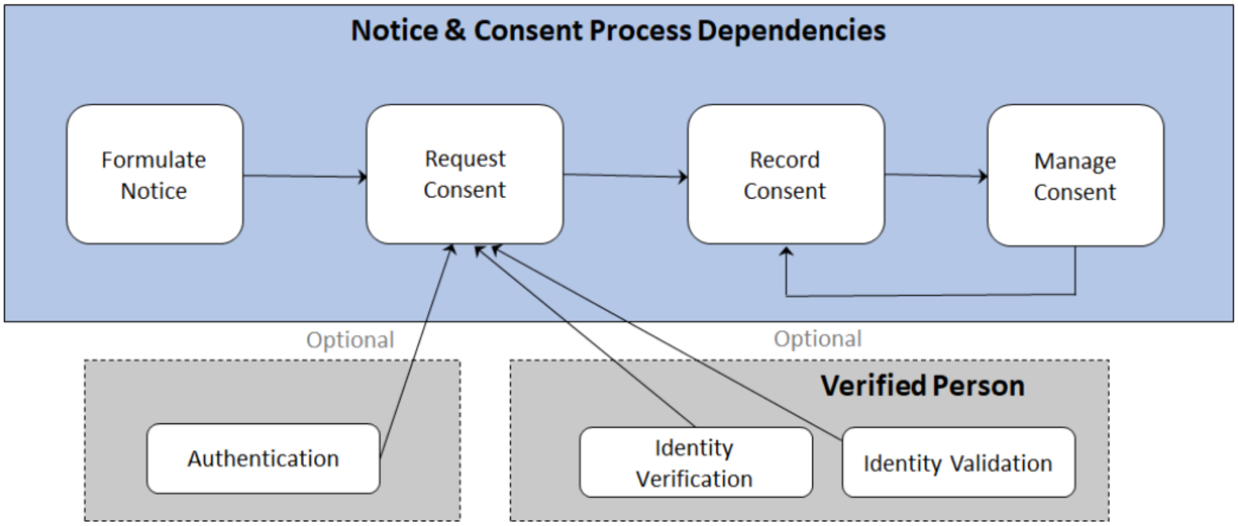

Figure 3. Trusted Process Dependencies

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 process may be the responsibility of one organization, and the Record Consent process 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. However, all approaches must respect relevant legislation, policy, and regulations.

  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**, 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/or consent may be required multiple times in a single digital identity flow. For example, a Subject may consent to share specific, limited information at the beginning of a transaction. Subsequently a Requesting Organization may discover that additional information is required in order to complete the transaction and that they must issue an additional request for consent to share that additional information. Additional notices and/or consent requests can also occur when a downstream process requires services from an additional party (not involved in the initial consent process) and consent to share information with that new party is required.

5 References

1. Government of Canada, Department of Justice. *Personal Information Protection and Electronic Documents Act (Canada). Schedule 1, Section 5*. <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-11.html>
2. Government of Canada, Department of Justice. *Official Languages Act (Canada).* <https://laws-lois.justice.gc.ca/eng/acts/o-3.01/>

6 Revision History

Version Number	Date of Issue	Author(s)	Description
0.01	2017-01-30	SECUREKEY	Initial working draft
0.02	2018-04-19	Consult Hyperion	First full draft
0.03	2018-04-26	Consult Hyperion	Addressed review comments
0.04	2019-03-25	PCTF Editor	Updated for discussion draft
0.05	2019-05-24	PCTF Editor	Incorporated comments from discussion draft open review
1.0	2019-08-07	TFEC, PCTF Editor	Component is now in the Draft Recommendation stage
1.1	2019-12-13	PCTF Editor	Updates from Open Review of the Draft Recommendation, apply standard PCTF component structure.
1.2	2020-02-10	PCTF Editor	Updates to incorporate feedback from the public review.
1.0	2020-05-11	PCTF Editor	Final Recommendation V1.0