Notice and Consent Component Overview

Document Version Control

0.1	2017-01-30	SECUREKEY	Initial working draft
0.2	2018-04-19	Consult Hyperion	First full draft
0.3	2018-04-26	Consult Hyperion	Addressed review comments

Table of Contents

Notice and Consent Component Overview

Overview

The Notice and Consent Component defines a set of processes used to formulate a statement and obtain a consent decision on that statement from a person authorized to do so. The Notice and Consent processes ensure that consent-requiring statements are accurately formulated according to defined requirements, 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 consent processes by means of standardized conformance criteria used for assessment and certification. Once a process is certified it becomes 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.

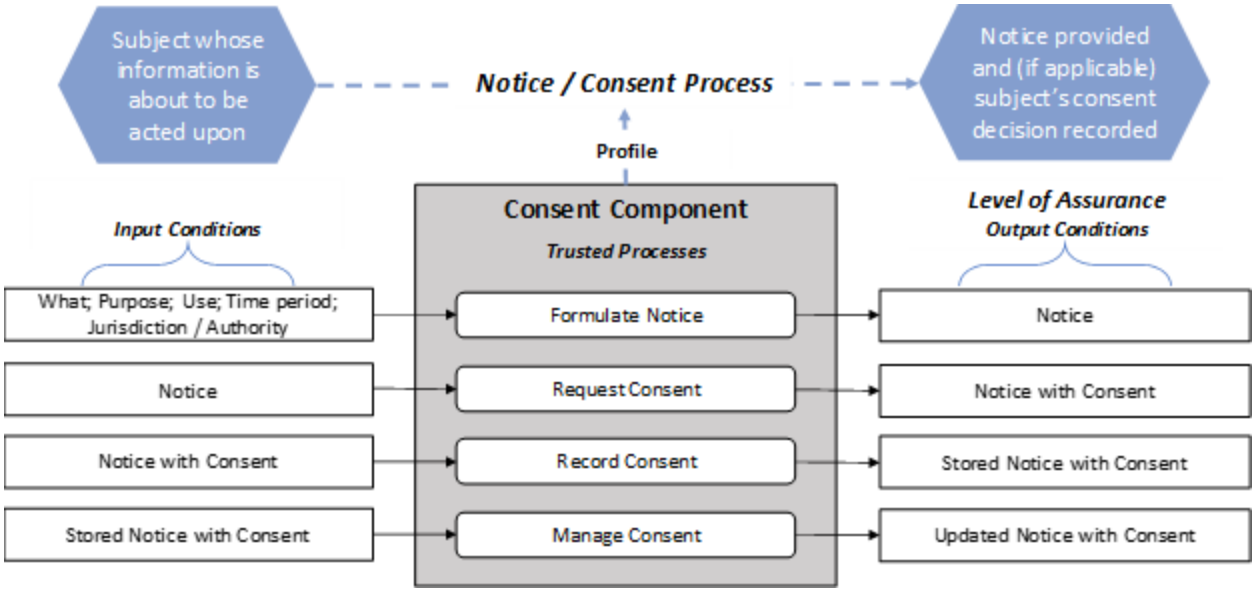

Figure 1 - Notice and Consent Component

The Notice and Consent Component consists of elements that indicate the following:

- **Trusted Processes** – the set of processes that conform to criteria (conformance criteria) 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 – a *state requiring consent to proceed*
- **Outputs** – output resulting from trusted processes – a *consent decision made by the subject*
- **Dependencies** – relationship between trusted processes
- **Profiles** – profiles used to ensure consistency of implementation, specify additional criteria, and facilitate *Pan-Canadian Trust Framework* certification.

Relationship to the Pan-Canadian Trust Framework

Figure 2 is an illustration of the *Pan-Canadian Trust Framework (Trust Framework)*. The Notice and Consent Component is a sub-component of *T rusted Digital Identity*.

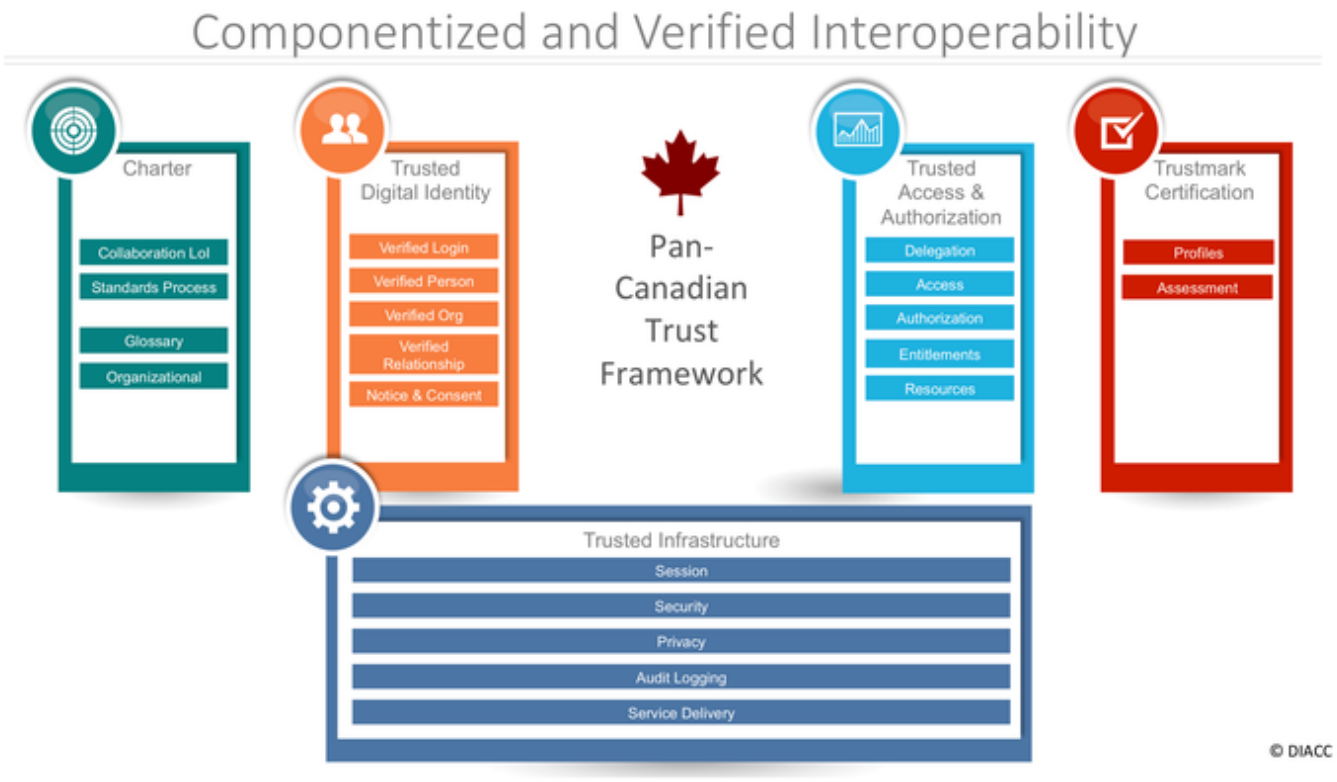

Figure 2: Pan-Canadian Trust Framework

Notice and Consent Trusted Processes

What is a Trusted Process?

A trusted process is a business or technical activity (or set of such activities) that transforms an input condition to an output condition. For example, a trusted process may be assigning a unique identifier to one and only one subject. Various controls are to be in place to ensure that this process has integrity, and that other trusted processes or services can rely upon this process.

Trusted processes are crucial to ensuring the integrity of access to digital services, to the overall integrity of the digital supply chain, and to the overall integrity of the Trust Framework. The integrity of a trusted process is paramount because the output or result of a trusted process is relied upon by many participants – across jurisdictional and sectoral boundaries, and, over the short term and long term. The Trust Framework ensures integrity of a trusted process through agreed upon and well-defined conformance criteria that support a transparent and evidence-based assessment methodology and certification process.

A business or technical process may be designated as a trusted process which is then assessed and certified according to conformance criteria stipulated by this Document and the Trust Framework. Figure 3 illustrates the model of *trusted process* having an *input condition*, an *output condition*, and in certain cases, a *dependency condition*.

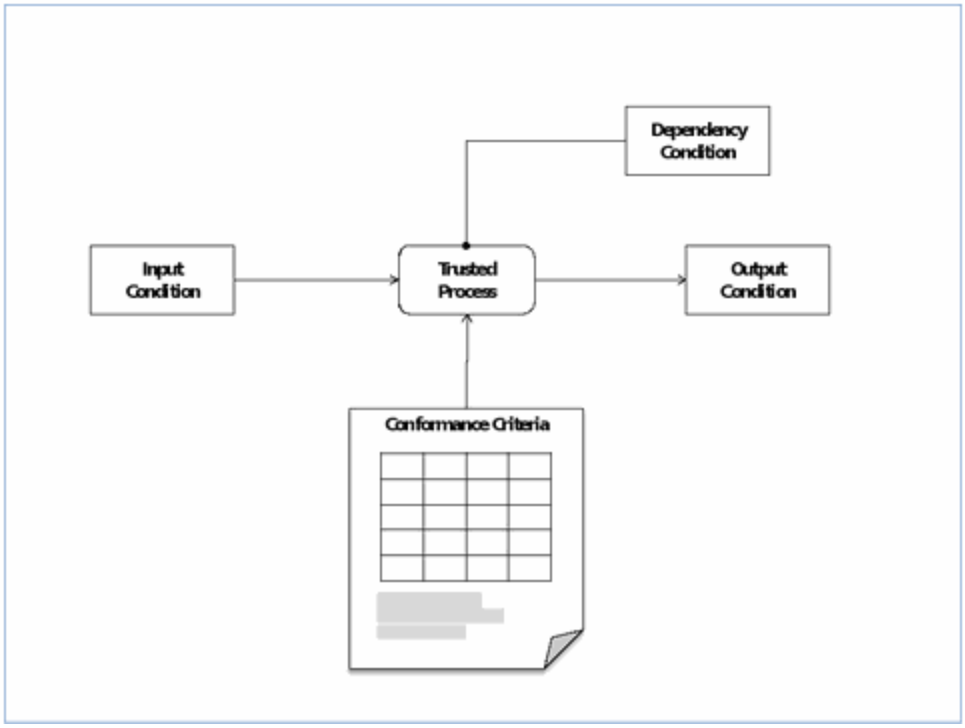

Figure 3: Trusted Process

A trusted process has *conformance criteria* specifying what is required to transform an *input condition* into an *output condition*; for example, for a *r equest consent process*, transforming from "*consent notice*" to "*consent decision*."

Overview of Notice and Consent Trusted Processes

The Notice and Consent Component defines four trusted processes:

1. Formulate Notice
2. Obtain Consent
3. Record Consent
4. Manage Consent

Formulate Notice

The Formulate Notice process establishes a statement that describes what personal information is being collected, used or disclosed; what the purpose is for the collecting, using or disclosing the information; with whom the information will be disclosed; how it will be handled and/or protected; the time period for which the notice will be applicable; and under whose Jurisdiction / Authority the notice is applicable. This statement is presented to the natural person in the form of a notice statement.

Request Consent

The Request Consent process will ensure that it is the subject (natural person to whom the personal information in question pertains) who is performing the action (on behalf of himself/herself) to indicate authority to make the consent decision. This will typically involve identifying and authenticating the subject using the Verified Person and Verified Login PCTF components.
The process to request consent of a subject includes presentation of the notice to the subject and providing a capability for the subject to impart a decision to provide consent or decline consent to the information in the notice, resulting in a consent decision.

Record Consent

The Record Consent process involves persisting (storing) the record of the notice conditions and the subject's consent decision, to storage. Notice conditions to be stored include, for example, information on the subject of the notice, the date/time of notice presentation, and the version of the notice presented. Consent decision conditions to be stored may 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, a notification on the consent decision made is issued to the relevant parties to the consent decision.

Manage consent

The processes required to manage the lifecycle of consent decisions include:

- **Update**: Updating a consent decision involves the subject establishing a revised consent decision from a previously stored consent decision. This could include the subject revoking the consent. This process results in an updated consent decision (which will need storing via the Record Consent process).
- **Review**: The process to review consent involves making the details of a stored consent decision visible to a reviewer.

Notice and Consent Conditions

What is a Condition?

A *condition* is a particular state or circumstance that is relevant to a trusted process. It may be an *input*, *output* and/or a *dependency* in relation to a trusted process.

Table 3 specifies the relevant conditions for the Notice and Consent Component.

Condition	Description
What; Purpose; Use; Time period; Jurisdiction / Authority	Specifics used to establish a statement for which the subject must consent in order to continue with the system process
Notice	The presentation of the consent statement that is crafted by the system to the subject / recognized authority
Notice with Consent	The selection (by the subject) to provide consent or decline consent
Stored Notice with Consent	The record of the notice and consent decision to a storage medium

Table 3: Notice and Consent Component Conditions

Levels of Assurance

Levels of assurance do not apply to the Notice and Consent Component in the same way that 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. Notice and consent requirements, however, apply across all levels – in particular there is no equivalent to “unverified” or “low assurance” notice and consent. Even at low levels consent should be obtained in broadly the same manner.

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

Dependencies

Some 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 5 specifies the *inputs*, *outputs*, and *dependencies* between the trusted processes of the Notice and Consent Component.

Trusted Process	Input	Dependency	Output
Formulate Notice	What; Purpose; Use; Time period; Jurisdiction / Authority	-	Notice
Request Consent	What; Purpose; Use; Time period; Jurisdiction / Authority	Formulate Notice	Notice with Consent
Record Consent	Consent notice	Request Consent	Stored Notice with Consent
Manage Consent	Consent decision	Record consent	Stored Notice with Consent

Table 5: Trusted Process Relationships

Notes and Assumptions

More than one organization may be responsible for carrying out the Notice and Consent trusted processes from end-to-end. It may be the case that several organizations may be carrying out the trusted processes (instead of just one organization). For example, request consent may be the responsibility of one organization, while record consent may be the responsibility of a different organization. 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 organisation, disclosing organisation 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.