Verified Login Component Overview Discussion Draft Version 0.06

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 Verified Login Component Overview

The Verified Login Component defines a set of processes used to enable access to digital systems and a set of conformance criteria for each process. These processes include binding a credential to a subject, binding authenticators to a credential, as well as lifecycle management functions that include updates, suspension, recovery, and revocation, and session management. For the purposes of Verified Login, a subject may be a person, organization, application, or device.

The objective of the Verified Login Component is to ensure the ongoing integrity of the login processes by applying standardized conformance criteria for assessment and certification. Verified Login is a set of processes that are intended to help establish confidence and trust in the use of a trusted digital identity. 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 Verified Login Component.

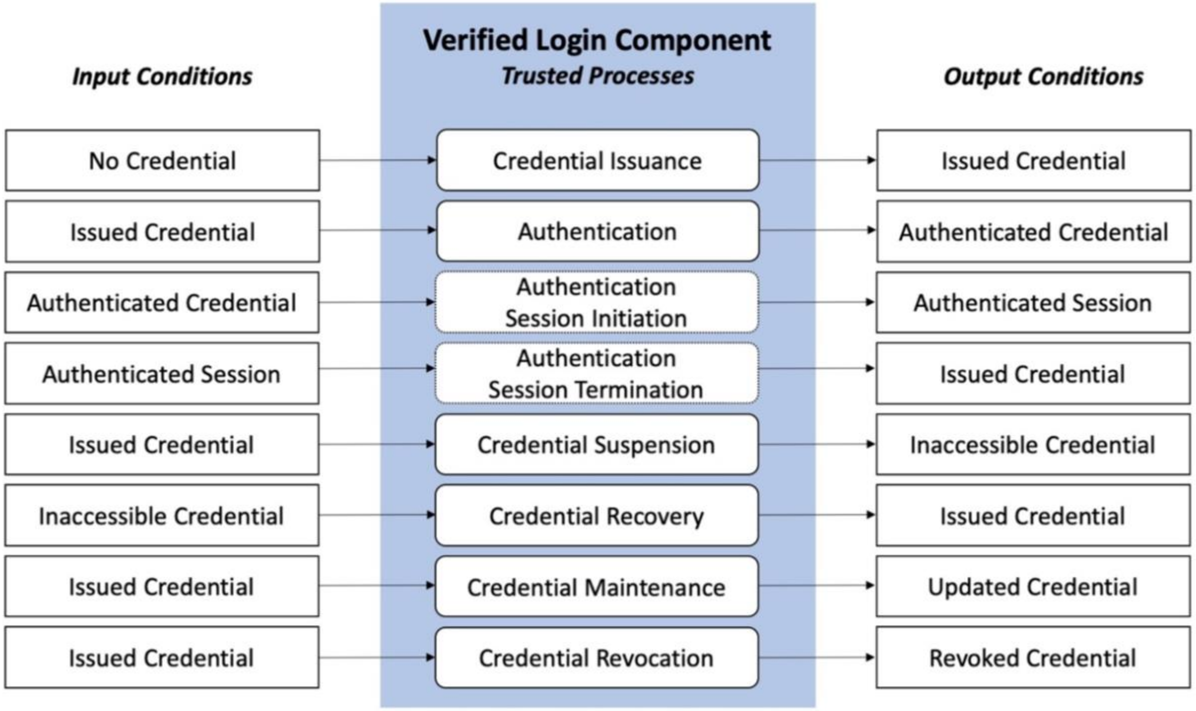

Figure 1. Verified Login Component

The Verified Login Component consists of elements that indicate the following:

- **Trusted Processes** – the set of processes that conform to criteria (i.e., 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 login.
- **Inputs** – input into Trusted Processes, for example, an issued credential.
- **Outputs** – output resulting from Trusted Processes, for example, an authenticated credential at a specific Level of Assurance.
- **Dependencies** – 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. 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 Model Visual Draft. The processes of the Verified Login Component are performed by participants in the Create & Manage Digital Identities as well as the Use Digital Identity categories.

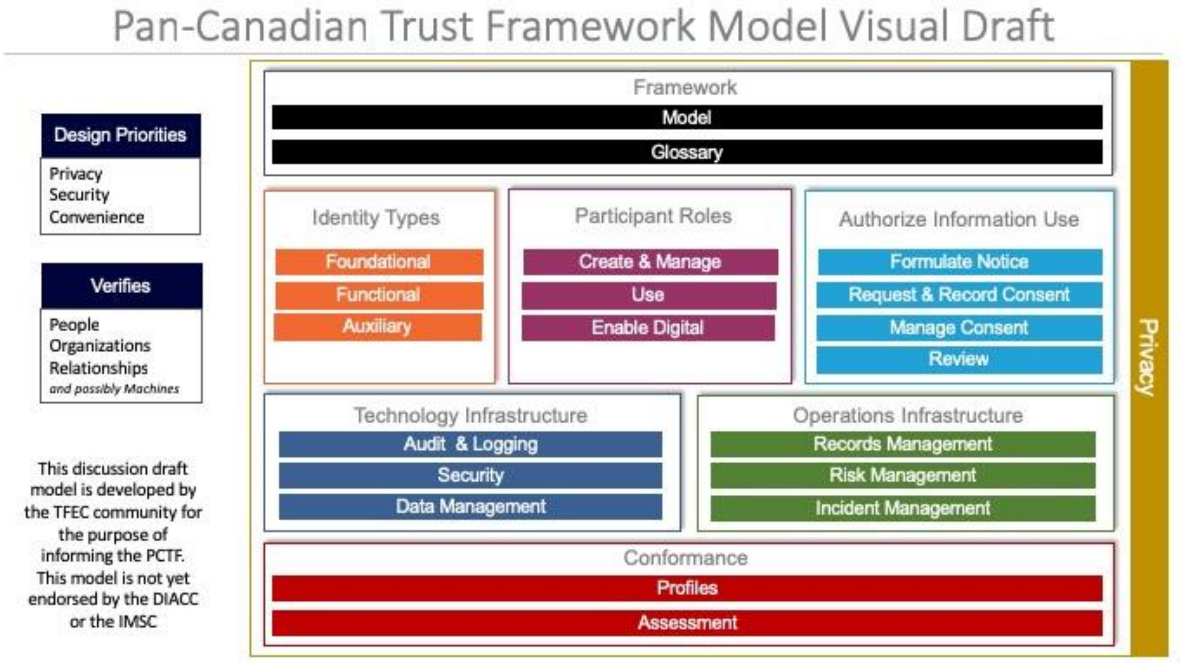

Figure 2. **Pan-Canadian Trust Framework Model Visual Draft**

2 Verified Login 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 Credential Issuance process to transform a “no credential” input condition to an “issued credential” output condition. A trusted Verified Login business or technical process is assessed and certified according to conformance criteria stipulated by the Verified Login Conformance Profile and the Pan-Canadian Trust Framework.

2.2 Verified Login Trusted Processes

The Verified Login Component defines eight Trusted Processes:

1. Credential Issuance
2. Authentication
3. Authentication Session Initiation
4. Authentication Session Termination
5. Credential Suspension
6. Credential Recovery
7. Credential Maintenance
8. Credential Revocation

2.2.1 Credential Issuance

Credential Issuance is an enrolment process, during which a credential is created and bound to one or more authenticators. The authenticators may be issued during this process, provided by the Subject, or provided by a third party. The authenticators will be subsequently used to prove, with the specified Level of Assurance, that a credential is referring to the same Subject that was originally bound to the credential. A credential includes one or more identifiers which may be pseudonymous, and may contain attributes verified by the credential issuer.

2.2.2 Authentication

Authentication is defined in the Pan-Canadian Assurance Model[1] as “The process of establishing truth or genuineness to generate an assurance”. It establishes the confidence, or Level of Assurance, that a Subject has control over their issued credential and that the credential is currently valid (i.e., not suspended or revoked).

2.2.3 Authentication Session Initiation

A session enables a persistent interaction between a Subject and an end-point, such as a credential provider or relying party, while removing the need to continuously repeat the authentication process between interactions. This Trusted Process is optional but may be required to satisfy certain use cases such as federation and single sign-on use cases. A session is started when a credential enters the Authenticated Credential state. The session is assigned a Level of Assurance that is equal to or lower than the Level of Assurance assigned to the corresponding credential; the session Level of Assurance must not be higher than the credential Level of Assurance.

2.2.4 Authentication Session Termination

The Authentication Session Termination process is required when login sessions are used. A session is terminated by an explicit logout event, session expiration due to inactivity or maximum duration, or other means.

2.2.5 Credential Suspension

This process transitions an issued credential to an inaccessible credential, and may be initiated by an end user action, system administrator, or automatically by the system. A suspended credential is prohibited from being passed to Relying Parties, ensuring the Subject is denied access.

2.2.6 Credential Recovery

The Credential Recovery process provides a means to transition an inaccessible credential to a usable state. The process may be triggered by an end user, system administrator, or automatically by the system. Examples include:

- An end user correctly answers their security questions and answers to reset a forgotten password;
- A system administrator releases a credential that was suspended due to inactivity; or
- After 24 hours the system automatically releases a credential that was suspended due to excess failed authentication attempts.

2.2.7 Credential Maintenance

The Credential Maintenance process includes life-cycle activities such as binding new authenticators, removing authenticators, and updating authenticators (e.g., password change, updating security questions and answers). This process is typically initiated by an end user but may also be initiated by a system administrator, or automatically by the system.

2.2.8 Credential Revocation

The Credential Revocation process ensures that a credential is permanently disabled or deleted. Once a credential is revoked, it can no longer be used. The system will actively prevent further Trusted Processes from occurring in relation to this credential. The process can be initiated by an end user, system administrator, or automatically by the system.

2.3 Verified Login Conditions

2.3.1 Input and Output Conditions

Table 1 specifies the input and output conditions for the Verified Login Component.

Condition	Description
No Credential	There is no credential assigned to the Subject.
Issued Credential	A credential has been bound to a single Subject, and appropriate authenticators have been bound.
Authenticated Credential	The Subject has successfully authenticated and proven control of the credential at the specified Level of Assurance.
Authentication Session	A persistent interaction between a Subject and an endpoint.
Inaccessible Credential	The Subject is currently not able to use the credential. This can be trigger by the Subject (e.g. forgotten password) or the system (e.g. lockout due to successive failed authentications, inactivity, suspicious activity, etc.). This is a temporary condition which will transition to an issued or revoked credential.
Updated Credential	The credential has been updated. This is a temporary condition which will transition to an issued or authenticated credential.
Revoked Credential	The credential is permanently disabled or deleted. This is a permanent condition.

Table 1. Verified Login 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 Verified Login Component.

Trusted Process	**Input Condition**	**Process Dependency**	**Output Condition**
Credential Issuance	No Credential	-	Issued Credential
Authentication	Issued Credential	Credential Issuance	Authenticated Credential
Authentication Session Initiation	Authenticated Credential	Authentication	Authentication Session
Authentication Session Termination	Authentication Session	Authentication Session Initiation	Issued Credential
Credential Suspension	Issued Credential	Credential Issuance	Inaccessible Credential
Credential Recovery	Inaccessible Credential	Credential Issuance	Issued Credential
Credential Maintenance	Issued Credential	Credential Issuance Authentication[2]	Updated Credential
Credential Revocation	Issued Credential	Credential Issuance Authentication[2]	Revoked Credential

Table 2. Trusted Process Relationships

3 Levels of Assurance

A Level of Assurance is a qualification that must be applied and maintained to indicate a level of confidence in the Verified Login Trusted Processes. It is used by Credential Providers, Relying Parties and end users to determine to what degree of confidence the access to a digital system should have given the context of the ensuing digital interaction.

The Level of Assurance (LOA) also indicates that the processes within the Verified Login Component have been assessed and/or certified in accordance with the Trust Framework Conformance Criteria. Table 3 lists the four levels of assurance defined in existing trust frameworks.

Level of Assurance	Qualification Description
Level 1 (LOA1)	· Little or no degree of confidence required · Satisfies Level 1 Conformance Criteria
Level 2 (LOA2)	· Some (reasonable) degree of confidence required · Satisfies Level 2 Conformance Criteria
Level 3 (LOA3)	· High degree of confidence required · Satisfies Level 3 Conformance Criteria
Level 4 (LOA4)	· Very high degree of confidence required · Satisfies Level 4 Conformance Criteria

Table 3. Levels of Assurance

Each Level of Assurance may be further refined by a qualifier. For example, a Relying Party in the health care sector may specify the requirement for an LOA3 credential, with a qualifier indicating the authenticator must be issued from a health care provider.

The resultant LOA of any Verified Login system is the lowest LOA associated with any of the seven Verified Login Trusted Processes. This principle is known as the “low water mark”. The requirements of each LOA are cumulative – successively higher LOA’s require that the requirements for lower LOA’s have been met as well.

4 Notes and Assumptions

More than one organization may be responsible for carrying out the Verified Login Trusted Process from end-to-end.

For example, Credential Issuance may be the responsibility of one organization, while Authentication 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.

Footnotes

[1] Pan-Canadian Assurance Model: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262&section=html

[2] The Authentication Process is a dependency when the process is initiated by an end user.