PCTF Verified Login Component Overview Draft Recommendation V1.0

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 for this Draft Recommendation are decision makers who may or may not be domain technology experts. When reviewing this draft, please consider the following and note that responses to these questions are non-binding and serve to improve the Pan-Canadian Trust Framework.

1. If your organization were to self-assess today, would you comply?
2. Could your organization comply?
3. Could your organization identify any barriers to compliance (business, legal, or technical)?
4. Would you be willing to complete a non-binding self-assessment? If so, would you be willing to share those results with the DIACC Trust Framework Expert Committee.
5. Is the description of the Trusted Processes clear and accurate?
6. Are the conformance criteria clear and measurable/assessible?
7. Do you agree with the terms used to describe Verified Login and the use of the phrase "Verified Login" for this component?
8. Do you agree with the removal of descriptive information from the conformance profile document and its consolidation in the overview document?
9. Do you agree with the re-structuring of the overview document to put all terms, definitions, roles, and other key information into a single section?

Contents

1 Introduction to the PCTF Verified Login Component

This document provides an overview of the PCTF Verified Login Component, a component of the Pan-Canadian Trust Framework (PCTF). For a general introduction to the PCTF, please see the PCTF Model Overview. The PCTF Model Overview provides the PCTF's goals and objectives, a high-level model outline of the PCTF, and contextual information.

Each PCTF component is made up of two documents:

1. Overview – Introduces the subject matter of the component. The overview 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 Verified Login Conformance Profile.

1.1 Scope

The PCTF Verified Login Component defines:

1. A set of processes that enable access to digital systems. Processes in scope for this component include binding a Credential to a Subject, binding Authenticators to a Credential, session management, and Credential lifecycle management functions (e.g., updates, suspension, recovery, and revocation).
2. A set of Conformance Criteria for each process that, when a process is shown to be compliant, enable the process to be trusted.

1.2 Purpose and Anticipated Benefits

The purpose of the PCTF Verified Login Component is to ensure the on-going integrity of login processes by applying standardized Conformance Criteria for process assessment and certification. The Conformance Criteria for this component may be used to ensure:

- Trusted Processes result in the representation of a unique Subject and a Level of Assurance that it is the same Subject with each successful login to an Authentication Service Provider.
- The reliability of Trusted Processes needed to maintain the integrity and security of the Authenticators used to gain access to remote systems.

All participants will benefit from:

- Repeatability and continuity in the login processes that they offer or on which they depend.
- Assurance that identified Users can engage in authorized interactions with remote systems.

Relying Parties benefit from:

- The ability to build on the assurance of the Verified Login Trusted Processes to uniquely identify a Subject within their application or program space.

1.3 Biometrics and Verified Login

Given the inherent lack of revocability of biometrics, industry standards relevant to this component generally regard biometrics as a means to unlock an Authenticator within a local device to facilitate remote Authentication with a service. An example of such a scenario is someone using Apple's TouchID or FaceID to unlock access to a mobile one-time passcode or other locally stored and generated mobile Authenticator.

- **NIST 800-63** describes the use of biometrics as follows: "A biometric also does not constitute a secret. Accordingly, these guidelines only allow the use of biometrics for authentication when strongly bound to a physical authenticator."
- **ITSP.30.031** describes the use of biometrics as follows: "Something a user is or does may be replicated. A threat actor may obtain a copy of the token owner's fingerprint and construct a replica - assuming that the biometric system(s) employed do not block such attacks by employing robust liveness detection techniques." and "Automated recognition of individuals based on their behavioural and biological characteristics. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration."

Based upon the above guidance from NIST and ITSP, this version of PCTF Verified Login Component considers biometric Authentication only in the context of unlocking access to another Authenticator, with the most popular example being unlocking access through biometric to a mobile Authenticator.

1.4 Relationship to the Pan-Canadian Trust Framework

The Pan-Canadian Trust Framework 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 1 is an illustration of the components of the draft Pan-Canadian Trust Framework.

Figure 1. Components of the draft Pan-Canadian Trust Framework

The benefits associated with the PCTF Verified Login Component are realized in part by expanding on processes defined in the PCTF Verified Person Component (and, to some extent, the PCTF Verified Organization Component). In this regard, the PCTF distinguishes between "verification" and "authentication" processes and recognizes that Authenticated Sessions remain necessary to ensure security and privacy online.

2 Verified Login Conventions

This section describes and defines key terms and concepts used in the PCTF Verified Login Component. This information is provided to ensure consistent use and interpretation of terms appearing in this overview and the PCTF Verified Login Conformance Profile.

For the purposes of this PCTF component:

- The term Login does not refer exclusively to a preferred authentication method (e.g., username/password) or technology (e.g., cryptographic keys vs. biometrics).
- The Trusted Processes defined for this component are agnostic with respect to how digital IDs are issued and managed. In this sense, digital IDs issued and managed using self-sovereign identity or more conventional issuance processes may take advantage of this component.

Note

- Conventions may vary between PCTF components. Readers are encouraged to review the conventions for each PCTF component they are reading.
- Defined Terms – Key terms and concepts described and defined in this section, the section on Trusted Processes, and the PCTF Glossary are capitalized throughout this document.

- Hypertext Links – Hypertext links may be embedded in electronic versions of this document. All links were accessible at time of writing.

2.1 Terms and Definitions

For purposes of this PCTF component, terms and definitions listed in the PCTF Glossary and the terms and definitions listed in this section apply.

Adaptive Risk

Dynamic measure of the risk associated with a transaction or service access based on context and behaviour.

Adaptive Risk Authentication

Dynamically adjusting the specific authentication steps performed according to the Adaptive Risk.

Authentication Factors

There are three Authentication Factors:

1. Something the Subject has
2. Something the Subject knows
3. Something the Subject is or does

Authenticator

Information or biometric characteristics under the control of an individual that is a specific instance of an Authenticator Type; the specific instance of the Authenticator Type that is under the control of the individual.

Examples:

1. Private signing key equal to 011011101010101011000101
2. Password that is equal to A$n45!R78oR
3. Person's face (note: the face image is captured and potentially further processed in preparation for analysis against authenticator validation data)

Authenticator Type

A class of authenticator within a specified authentication factor.

Examples:

1. Crypto keys & RSA one-time-password (OTP) token – Something you have
2. Passwords & knowledge-based authentication (KBAs, e.g., responses to challenge questions) – Something you know

3. Fingerprints, retinas, keyboard stroke timing, gait – Something you are

Authenticator Validation Data

Data under the control of a service provider against which the authenticator (provided by a Subject during an authentication attempt) is validated.

Examples:

1. Public signature validation key (associated with Subject private key) equal to 001001101010111111010000
2. Hash of Subject's password A$n45!R78oR or current state of a one-time password (OTP) generator
3. Subject's enrolment facial image (or biometric template of Subject's enrolment facial image, depending on what is stored by the Credential Service Provider)

Credential

Data that uniquely binds Authenticator Validation Data to identity data. For the purposes of this PCTF component, "Credential" only refers to digital data structures.

Examples:

1. Subject's driver's license number (plus possibly other data record pointers) binds the Subject's transport ministry identity record to the Subject's face image/biometric template in transport ministry's biometric database
2. Subject's bank account number binds the Subject's identity data at the bank with the hash of the Subject's bank account password

Independently Audited
The referenced audit must be performed by an audit group that is unconnected to, discrete from, or otherwise not part of the business unit responsible for the process or activity that is the subject of the audit.

IT Service Management
The entirety of activities – directed by policies, organized and structured in processes and supporting procedures – that are performed by an organization to design, plan, deliver, operate and control information technology services offered to customers.

Note

- See Appendix A for an example use case that illustrates how some of the above terms are used in the PCTF Verified Login Component.

2.2 Abbreviations

The following abbreviations and acronyms appear throughout this overview and the PCTF Verified Login Conformance Profile:

- DIDs – Decentralized Identifier(s)
- IETF – Internet Engineering Task Force
- IT – Information technology
- ITIL – Information Technology Infrastructure Library
- ITSP – IT Security Guidance for Practitioners
- LOA(s) – Level(s) of Assurance
- NIST – National Institute of Standards and Technology
- OTP – One-time password
- PCTF – Pan-Canadian Trust Framework
- Q&A – Question(s) and Answer(s)
- TLS – Transport Layer Security
- W3C – World Wide Web Consortium

2.3 Roles

The following roles and role definitions are applicable in the scope and context of the PCTF Verified Login Component. These roles help to isolate the different functions and responsibilities within the end-to-end Verified Login Trusted Processes.

Note

- Depending on the use case, different organizations may assume one or multiple roles. For example, Credential Issuance may be the responsibility of one organization, while Authentication may be the responsibility of a different organization.
- Role definitions do not imply or require any particular solution, architecture, or implementation or business model.

Authentication Service Provider

An entity that operates a service that implements the Verified Login Trusted Processes related to authentication:

1. Authentication
2. Authentication Session Initiation (optional)
3. Authentication Session Termination (optional)

Credential Service Provider

An entity that operates a service that implements the Verified Login Trusted Processes related to credential management:

1. Credential Issuance
2. Credential Suspension

3. Credential Recovery
4. Credential Maintenance
5. Credential Revocation

Relying Party

An entity that depends on a conforming implementation of the Verified Login Trusted Processes.

Subject

A Subject may be a natural person, an organization, an application, or a device bound to a credential.

2.4 Levels of Assurance

A Level of Assurance is an indicator that must be applied and maintained to describe a level of confidence in the PCTF Verified Login Component Trusted Processes. In the context of this PCTF component, Credential Providers, Relying Parties, and Users use LOAs to determine what degree of confidence the access to a digital system should have given the context of the ensuing digital interaction. A LOA also indicates that Verified Login processes have been assessed and/or certified in accordance with the PCTF Verified Login Conformance Criteria.

For this PCTF component, Conformance Criteria are profiled in terms of LOA; the conformance criteria explicitly list the requirements for each LOA of a process. They specify the requirements and relative stringency of the requirements that must be met to attain a given LOA for a process. It is necessary to comply with all Conformance Criteria for a given LOA for all processes to attain that Level of Assurance. The resultant LOA of any Verified Login system is the lowest LOA associated with any of the Verified Login Trusted Processes. The requirements of each LOA are cumulative – successively higher LOA's require that the requirements for lower LOA's have been met as well.

Table 1 lists the four Levels of Assurance defined for the PCTF Verified Login Component.

	Level of Assurance	Qualification Description
280-a	Level 1 (LOA1)	• Little or no degree of confidence required • Satisfies Level 1 Conformance Criteria
280-b	Level 2 (LOA2)	• Some (reasonable) degree of confidence required • Satisfies Level 2 Conformance Criteria
280-c	Level 3 (LOA3)	• High degree of confidence required • Satisfies Level 3 Conformance Criteria
280-d	Level 4 (LOA4)	• Very high degree of confidence required • Satisfies Level 4 Conformance Criteria

Table 1. Levels of Assurance

Note

- This version of the PCTF Verified Login Component does not define Conformance Criteria for LOA 4. However, the PCTF acknowledges the existence of LOA 4 and has included it as a placeholder for future versions.
- Each LOA may be further refined by a qualifier. For example, a Relying Party in the health care sector may specify in a PCTF Profile a requirement for an LOA3 Credential with a qualifier that the authenticator must be issued by a health care provider.

3 Trusted Processes

The PCTF promotes trust through a set of auditable business and technical requirements for various defined processes.

A process is a business or technical activity (or set of such activities) that transforms an input condition to an output condition – an output on which other processes often depend. A condition is a particular state or circumstance that is relevant to a Trusted Process. It may be an input, output, or dependency in relation to a Trusted Process. Conformance Criteria specify what is required to transform an input condition into an output condition. Conformance Criteria specify, for example, what is required for the Credential Issuance process to transform a “No Credential” input condition to an “Issued Credential” output condition.

In the PCTF context, a process is designated a Trusted Process when it is audited and certified as conforming to Conformance Criteria defined in a PCTF conformance profile. The integrity of a Trusted Process is paramount because many participants—across jurisdictional, organizational, and sectoral boundaries and over the short-term and long-term—rely on the output of that process.

The PCTF Verified Login Component defines eight Trusted Processes:

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

A Verified Login process is designated a Trusted Process when it is audited and certified according to Conformance Criteria stipulated by the PCTF Verified Login Component Conformance Profile. Conformance Criteria specified in other PCTF components of may also be applicable under certain circumstances.

3.1 Conceptual Overview

Figure 2 provides a conceptual overview and the logical organization of the PCTF Verified Login Component Trusted Processes.

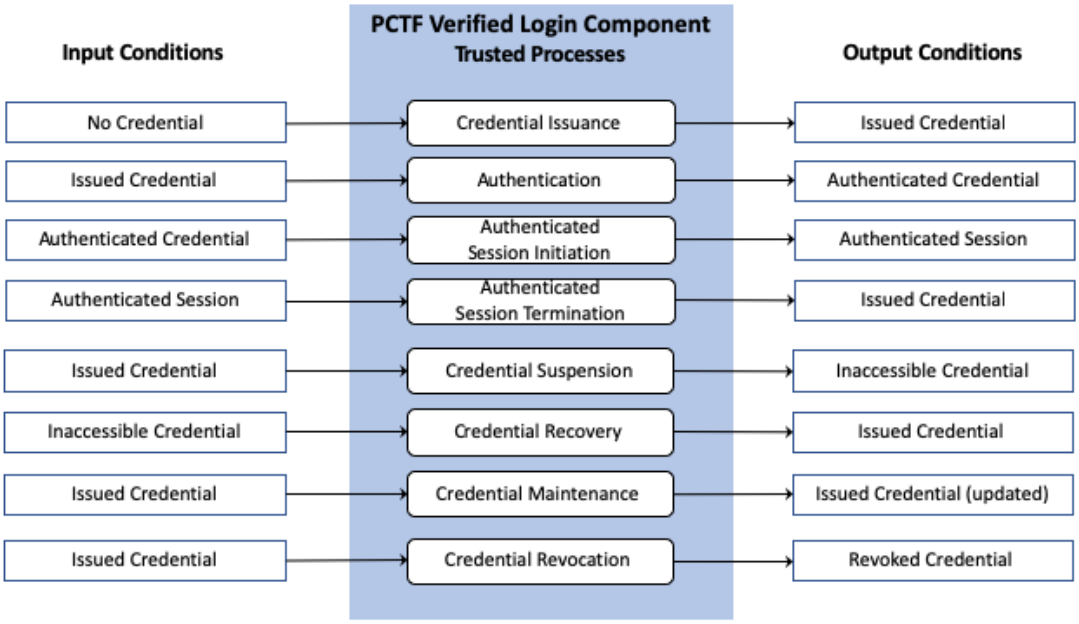

Figure 2. Verified Login Component Conceptual Overview

3.2 Process Descriptions

The following sections define PCTF Verified Login Component Trusted Processes. The PCTF Verified Login Conformance Profile specifies the Conformance Criteria against which the trustworthiness of these processes can be assessed.

Verified Login Trusted Processes are defined using the following information:

1. Description – A descriptive overview of the process (the opening paragraphs)
2. Inputs – What is put in, taken in, or operated on by the process
3. Outputs – What is produced by or results from the process
4. Dependencies – Related Trusted Processes, primarily those that produce outputs on which the process depends

Note

- Inputs and outputs are both types of conditions (conditions being particular states or circumstances that are relevant to a Trusted Process). In this section, the input and output conditions are relevant to Verified Login.

3.2.1 Credential Issuance

Credential Issuance is an enrolment process, during which a Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject. 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.

Note

- Validation and verification of the Subject's identity are not part of this process. The validation and/or verification of the Subject's identity when required is addressed by processes in the PCTF Verified Person Component.

Inputs	No Credential – There is no Credential assigned to the Subject.
Outputs	Authenticated Session – A persistent interaction between a Subject and an end-point.
Dependencies	Authentication

3.2.2 Authentication

Authentication is defined in the Government of Canada's Guideline on Defining Authentication Requirements (section 1.3) [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). In the event of a revoked or suspended Credential, the output would be a Revoked Credential or Inaccessible Credential, respectively, as the Credential Revocation or Credential Suspension processes would be invoked.

Inputs	Issued Credential – A Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
Outputs	Authenticated Credential – The Subject has successfully authenticated and proven control of the Credential at the specified LOA.
Dependencies	Credential issuance

3.2.3 Authenticated Session Initiation

A persistent interaction is a session between a Subject and an end-point, such as a Credential provider or Relying Party. A session may be required, for example, to satisfy federation and single sign-on (SSO) use cases. This Trusted Process is optional.

Authenticated Session Initiation must begin with an Authenticated Credential. The output of the Authenticated Session Initiation is an Authenticated Session, which is persistent interaction between Subject and end-point. If the authentication process conforms to LOA2, then the

Authenticated Session must be considered LOA2. If the authentication process conforms to LOA3, then the Authenticated Session must be considered LOA3.

Inputs	Authenticated Credential – The Subject has successfully authenticated and proven control of the Credential at the specified LOA.
Outputs	Authenticated Session – A persistent interaction between a Subject and an end-point.
Dependencies	Authentication

3.2.4 Authenticated Session Termination

The Authenticated Session Termination process is required when login sessions are used. An Authenticated Session is terminated through such events as an explicit logout event, session expiration due to inactivity or maximum duration, or other means.

Inputs	Authenticated Session – A persistent interaction between a Subject and an end-point.
Outputs	Issued Credential – A Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
Dependencies	Authenticated Session Initiation

3.2.5 Credential Suspension

This process transitions an Issued Credential to an Inaccessible Credential and may be initiated by a User action, system administrator, or automatically by the system. An Inaccessible Credential is prohibited from use for authentication purposes.

Inputs	Issued Credential – A Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
Outputs	Inaccessible Credential – The Subject is currently not able to use the Credential. This can be triggered by the Subject (e.g., forgotten password) or the system (e.g., lockout due to successive failed attempts to authenticate, inactivity, suspicious activity). This is a temporary condition which will transition to an issued or revoked Credential.
Dependencies	Credential Issuance

3.2.6 Credential Recovery

The Credential Recovery process provides a means to transition an Inaccessible Credential to an Issued Credential. The process may be triggered by a User, system administrator, or automatically by the system.

Inputs	Inaccessible Credential – The Subject is currently not able to use the Credential. This can be triggered by the Subject (e.g., forgotten password) or the system (e.g., lockout due to successive failed attempts to authenticate, inactivity, suspicious activity). This is a temporary condition which will transition to an issued or revoked Credential.
Outputs	Issued Credential – A Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
Dependencies	Credential Issuance

3.2.7 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), or updating Credential attributes. This process is typically initiated by a User, but may also be initiated by a system administrator, or automatically by the system.

Inputs	Issued Credential – A Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
Outputs	Issued Credential (updated) – A Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
Dependencies	Credential Issuance Authentication [2]

3.2.8 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 a User, system administrator, or automatically by the system. Note that a new Credential can be issued for the same Subject. Re-issue equates to revoking a Credential and issuing a new Credential for the same Subject.

Inputs	Issued Credential – A Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
Outputs	The Credential is permanently disabled or deleted. This is a permanent condition.
Dependencies	Credential Issuance Authentication [2]

4 References

This section lists all external standards, guidelines, and other documents referenced in this PCTF component.

Note

- Where applicable, only the version or release number specified herein applies to this PCTF component.

Instead of developing entirely new standards, the PCTF Verified Login Component builds on and leverages the experience and lessons of organizations outside of DIACC that have developed or are evolving related processes and standards.

The PCTF Verified Login Component has taken guidance from and is based in part on the following standards and guidance documents:

1. ITSP.30.031 v3 User Authentication Guidance for Information Technology System (ITSP.30.031)
2. NIST 800-63-3 Digital Identity Guidelines (800-63-3, 800-63A, 800-63B, and 800-63C)
3. Good Practice Guide No. 44 Authentication and Credentials for use with HMG Online Service (GPG-44)

This PCTF component references the following items for exemplary, informational, or illustrative purposes:

1. CSEC ITSG-33
2. FIPS 140-2

5 Notes

1. Source: Government of Canada, Guideline on Defining Authentication Requirements. 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 a User.

Appendix A: Authentication Use Case

Scenario

Bank authentication for login to government service using bank login (authentication device not known (e.g., browser not known)); bank card number, password, OTP to known address (e.g., cellphone number, email address).

In this scenario...

Authentication factors are:

1. Something you know
2. Something you have

Authenticator types are:

1. (something you know): password
2. (something you have):
    1. OTP to known address
    2. authentication device (e.g., browser) (used in the validation process, but not useful in this example since the browser is not known)

Authenticators are:

1. Subject's actual password
2. Subject's browser – identified with browser fingerprint
3. Access to the known address of the Subject (e.g., access to email account of known email address, access to cellphone of known cellphone number, access to physical mailbox)
4. OTP (as a mechanism to authenticate possession of the known cellphone)

Authenticator validation data is:

1. Browser fingerprint data (for browser that was previously used by Subject)
2. Hash of Subject's actual password
3. Known address that was used for OTP distribution to the Subject
4. Hash of OTP generated during the authentication event (where OTP was sent to cellphone)

The credential:

1. Bank account number (reference to customer information file with identity data)
2. Reference that links the bank account number to the Subject's authenticator validation data

Appendix B: Summary of Trusted Process Conditions

Table 2 summarizes the input and output conditions of the PCTF Verified Login Component.

Condition	Description
No Credential	There is no credential assigned to the Subject.
Issued Credential	A Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
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 end-point.
Inaccessible Credential	The Subject is currently not able to use the Credential. This can be triggered by the Subject (e.g., forgotten password) or the system (e.g., lockout due to successive failed attempts to Authenticate, inactivity, suspicious activity). This is a temporary condition which will transition to an issued or revoked Credential.
Revoked Credential	The Credential is permanently disabled or deleted. This is a permanent condition.

Table 2. Verified Login Component Conditions

Appendix C: Summary of Trusted Process 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 3 summarizes the inputs, outputs, and dependencies between the Trusted Processes of the PCTF Verified Login Component.

513-a	**Trusted Process**	**Input Condition**	**Process Dependency**	**Output Condition**
513-b	**Credential Issuance**	No Credential	-	Issued Credential
513-c	**Authentication**	Issued Credential	Credential Issuance	Authenticated Credential
513-d	**Authenticated Session Initiation**	Authenticated Credential	Authentication	Authenticated Session
513-e	**Authenticated Session Termination**	Authenticated Session	Authenticated Session Initiation	Issued Credential
513-f	**Credential Suspension**	Issued Credential	Credential Issuance	Inaccessible Credential
513-g	**Credential Recovery**	Inaccessible Credential	Credential Issuance	Issued Credential
513-h	**Credential Maintenance**	Issued Credential	Credential Issuance Authentication[2]	Issued Credential (updated)
513-i	**Credential Revocation**	Issued Credential	Credential Issuance Authentication[2]	Revoked Credential

Table 3. Trusted Process Relationships