PCTF Authentication Component Overview

Document Status: Final Recommendation V1.1

In accordance with the DIACC Operating Procedures, Final Recommendations are 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 has been developed by DIACC's Trust Framework Expert Committee. 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.

Table of Contents

1. Introduction to the PCTF Authentication Component

This document provides an overview of the PCTF Authentication 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 Authentication Conformance Profile.

1.1 Scope

The PCTF Authentication Component defines:

1. A set of processes that enable access to digital systems.
2. A set of Conformance Criteria for each process that, when a process is shown to be compliant, enable the process to be trusted.

Note: The PCTF Authentication Component Trusted Processes defined for this component are agnostic with respect to how digital IDs are issued and managed at the technology level. Each Participant will need to determine which technologies and methods are best suited to the requirements of their constituents and their own target business outcomes.

1.2 Purpose and Anticipated Benefits

The purpose of the PCTF Authentication Component is to assure the on-going integrity of login and authentication processes by certifying, through a process of assessment, that they comply with standardized Conformance Criteria. The Conformance Criteria for this component may be used to provide assurances:

- That Trusted Processes result in the representation of a unique Subject at a Level of Assurance that it is the same Subject with each successful login to an Authentication Service Provider.

- Concerning the predictability and continuity in the login processes that they offer or on which they depend.

All participants will benefit from:

- Login and authentication processes that are repeatable and consistent (whether they offer these processes, depend on them, or both).
- Assurance that identified Users can engage in authorized interactions with remote systems.

Relying Parties benefit from:

- The ability to build on the assurance that Authentication Trusted Processes uniquely identify, at an acceptable level of risk, a Subject in their application or program space.

1.3 Biometrics and Authentication

Industry standards relevant to this PCTF component generally do not recommend the use of biometrics as the only Authentication Factor in a given system. Rather, current guidance suggests an appropriate use of biometrics is a means to unlock a local Authenticator (perhaps existing on a local device) to facilitate Authentication to a remote service:

- The US National Institute of Standards and Technology (NIST) publication **800-63-3 (Digital Identity Guidelines) (revision 3)** 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."
- The Communications Security Establishment publication **Information Technology Security Guidance for the Practitioner 30.031 V3 (User Authentication Guidance for Information Technology Systems)** 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 "Biometrics: 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."

This version of PCTF Authentication Component aligns with this guidance and considers biometric authentication appropriate only in combination with another authentication factor. An example of such a scenario is someone using Apple's TouchID or FaceID to unlock an iPhone depends upon that person having control and possession of the iPhone (something you have) and control and possession of a matching biometric (something you are).

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.

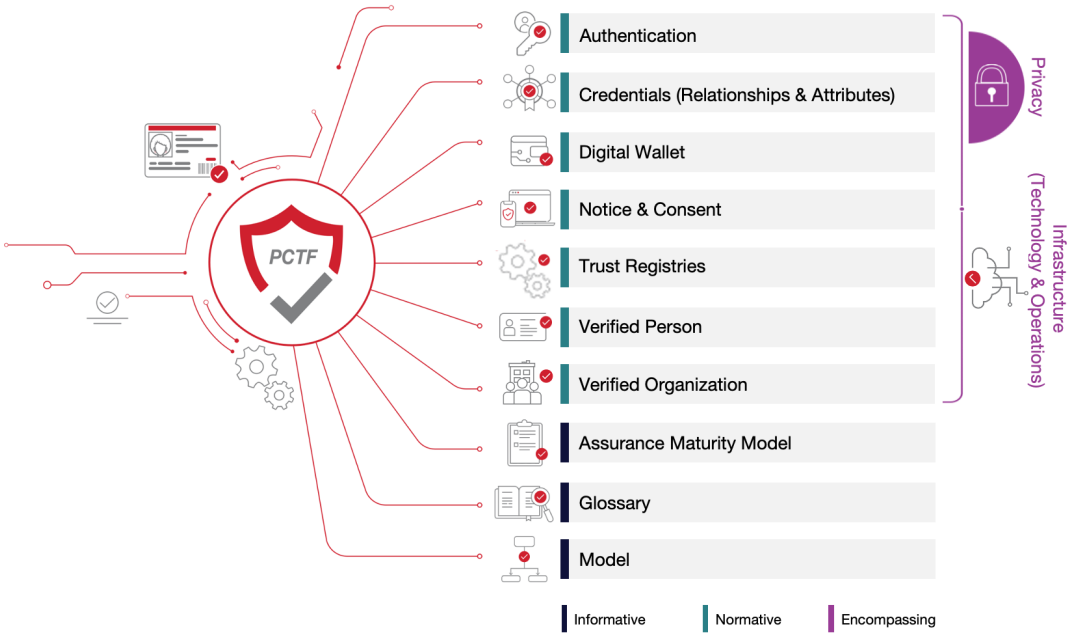

Figure 1. Components of the Pan-Canadian Trust Framework

The benefits associated with the PCTF Authentication 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. Authentication Conventions

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

For the purposes of this PCTF component:

- The terms "login" and "authentication" do not assume a preferred authentication method (e.g., username/password) or technology (e.g., cryptographic keys vs. biometrics).
- Successful login to a given system does not guarantee the integrity of data held by that system.
- The Trusted Processes defined for this component are agnostic with respect to how digital IDs are issued and managed. As a result, this component also provides relevant guidance for digital IDs issued and managed using decentralized identity or centralized identity issuance processes.

Notes:

- 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

Authentication is the process of establishing truth or genuineness to generate an assurance that a Subject has control over an Issued Authentication Credential and that the Authentication Credential is currently valid.

Authentication Factors

There are three Authentication Factors:

1. Something the Subject has (e.g., key card, key fob)

2. Something the Subject knows (e.g., password)
3. Something the Subject is or does (e.g., a biometric)

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.

An Authenticator may be provided by the Subject or by a service provider.

Authenticator Type

A class of authenticator within a specified authentication factor.

Authenticator Validation Data

Data under the control of an Authentication Service Provider against which the Authenticator (provided by a Subject during an authentication attempt) is validated. Refer to Appendix A for examples.

Credential

A data structure that uniquely binds at least one Authenticator to at least one claim about at least one Subject.

For the purposes of this PCTF component, a Credential refers to any Subject-bound data that is used in any of the Trusted Processes described herein.

Authenticator Binding

The association of one or more claims about a Subject with one or more Authenticators as part of the Credential Issuance process.

Inaccessible Credential

A Credential which is not accessible/available or exists in an incomplete state. This can occur as a result of an incomplete process or the Credential Suspension process.

Independently Audited

The referenced audit must be performed by an audit group that is not connected to, is discrete from, or is 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.

Session and Authenticated Session

A Session is a persistent interaction between a Subject's software agent (e.g., web browser, mobile app) and a software service used by service providers or Relying Parties. A Session may be required to satisfy federation and single sign-on (SSO) use cases.

An Authenticated Session is a Session (a persistent interaction between a Subject's software agent (e.g., web browser, mobile app) and a software service used by service providers or Relying Parties) that is securely linked to successful authentication of the Subject.

Subject

The Entity bound to a Credential. For the purposes of this PCTF component, the term Subject is only applied to Entities so bound. A Subject may be a natural person, an organization, an application, or a device.

Note: See Appendix A for an example use case that illustrates how some of the above terms are used in the PCTF Authentication Component.

2.2 Abbreviations

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

- DIDs – Decentralized Identifier(s)
- FIPS – Federal Information Processing Standards
- IETF – Internet Engineering Task Force
- IT – Information technology
- ITSG – Information Technology Security Guidance
- 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

Roles help to isolate the different functions and responsibilities that participants may perform within the end-to-end Authentication processes. Roles do not imply or require any particular solution, architecture, or implementation or business model.

Notes:

- 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 Authentication 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 Authentication Trusted Processes related to management of Credentials:

1. Credential Issuance
2. Credential Suspension (optional)
3. Credential Recovery (optional)
4. Credential Maintenance
5. Credential Revocation

Relying Party

An Organization or Person who consumes digital Identity Information created and managed by Participants to conduct digital transactions with Subjects. Note that in the context of this PCTF component, the Relying Party is consuming Credentials or an Authenticated Session from the Authentication Trusted Processes.

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 Authentication Component Trusted Processes. In the context of this PCTF component, Credential Service 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.

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 Authentication system is the lowest LOA associated with any of the Authentication Trusted Processes.

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

	Level of Assurance	Qualification Description
298b	Level 1 (LOA1)	• Little or no degree of confidence required • Satisfies Level 1 Conformance Criteria
298c	Level 2 (LOA2)	• Some (reasonable) degree of confidence required • Satisfies Level 2 Conformance Criteria
298d	Level 3 (LOA3)	• High degree of confidence required • Satisfies Level 3 Conformance Criteria
298e	Level 4 (LOA4)	• Very high degree of confidence required • Satisfies Level 4 Conformance Criteria

Table 1. Levels of Assurance

Notes:

- This version of the PCTF Authentication Component does not define Conformance Criteria for LOA4. However, the PCTF acknowledges the existence of LOA4 and has included it as a placeholder for future versions.
- Each LOA may be further refined by additional control requirements specific to their industry or service type. For example, a Relying Party in the health care sector may specify in a PCTF Profile a requirement for an LOA3 Credential with a criteria that the authenticator must be issued by a health care provider. Regardless of further refinement, however, additional criteria may never remove or reduce the obligation to meet the criteria specified in this profile.
- The resultant LOA is defined by the conformance criteria.

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 assessed 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 Authentication 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

An Authentication process is designated a Trusted Process when it is assessed and certified compliant with Conformance Criteria stipulated by the PCTF Authentication Component Conformance Profile. Conformance Criteria specified in other PCTF components may also be applicable under certain circumstances.

3.1 Conceptual Overview

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

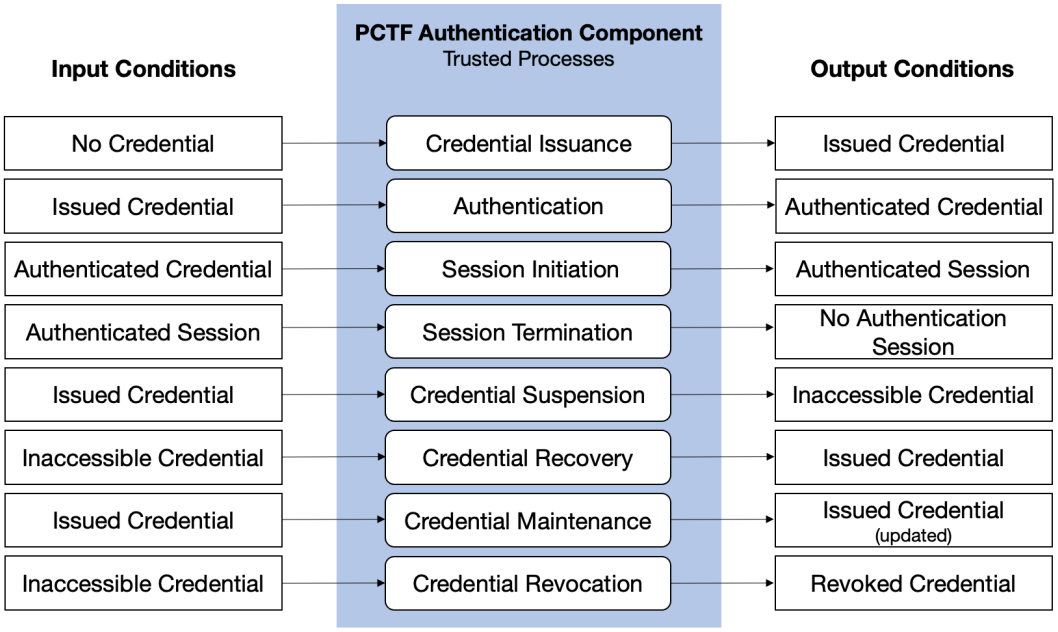

Figure 2. Authentication Component Conceptual Overview

3.2 Process Descriptions

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

Authentication 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 the PCTF Authentication Component.
- See Appendix B for a summary of the input and output conditions of the PCTF Authentication Component.

3.2.1 Credential Issuance

Credential Issuance is a process during which an Credential is issued, describing one or more Subjects, and bound to one or more appropriate Authenticators controlled by the

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

Note: Validation and Verification of Subject identity may be necessary to ensure an Authentication Credential is issued to the correct Subject or a known Subject. This is particularly true for Entities issuing and managing Authentication Credentials at LOA3 or higher. Please refer to the PCTF Verified Person Component for a description of Identity Validation and Verification processes and associated Conformance Criteria.

375a	**Inputs**	No Credential – There is no Credential assigned to the Subject.
375b	**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.
375c	**Dependencies**	

3.2.2 Authentication

Authentication is the process of establishing truth or genuineness to generate an assurance. With respect to this component, Authentication establishes, at a Level of Assurance, that a Subject has control over an Issued Authentication Credential and that the Authentication Credential is currently valid (i.e., not suspended or revoked). In the event of a revoked or suspended Authentication Credential, the output would be a Revoked Authentication Credential or Inaccessible Authentication Credential, respectively, as the Authentication Credential Revocation or Authentication Credential Suspension processes would have been enacted.

Note: In some cases, authentication may be bi-directional, with each party seeking to authenticate that the other party is genuine also (e.g., opening an online bank account and providing personal information). As appropriate, assessors should assess each direction against all applicable criteria.

389a	**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.
389b	**Outputs**	Credential – The Subject has successfully authenticated and proven control of the Credential at the specified LOA.
389c	**Dependencies**	Credential Issuance

3.2.3 Authenticated Session Initiation

An Authentication Session Initiation is a process that, given an Authenticated Credential, creates a secure session for a persistent interaction.

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

This process is optional and may not be supported by all service providers.

397a	**Inputs**	Authenticated Credential – The Subject has successfully authenticated and proven control of the Credential at the specified LOA.
397b	**Outputs**	Authenticated Session – A persistent interaction between a Subject's software agent (e.g., web browser, mobile app) and a software service used by service providers or Relying Parties that is securely linked to successful Authentication of the Subject.
397c	**Dependencies**	Authentication

3.2.4 Authenticated Session Termination

The Authenticated Session Termination is a process that, given an Authenticated Session, cancels that session (i.e., makes the Authenticated Session unusable for further communications). Session terminations may be triggered through such events as an explicit logout event, Session expiration due to inactivity or maximum duration, or other means.

This process is optional and may not be supported by all service providers.

405a	**Inputs**	Authenticated Session – A persistent interaction between a Subject's software agent (e.g., web browser, mobile app) and a software service used by service providers or Relying Parties that is securely linked to successful Authentication of the Subject.
405b	**Outputs**	No Authenticated Session
405c	**Dependencies**	Authenticated Session Initiation

3.2.5 Credential Suspension

The Credential Suspension is a process that converts an Issued Credential to an Inaccessible Credential and may be initiated by User action, system administrator, or

automatically by the system. An Inaccessible Credential should not be used in the Authentication process.

This process is optional and may not be supported by all service providers.

412a	**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.
412b	**Outputs**	Inaccessible Credential – The Subject is currently not able to use the Credential. This can be triggered by the Subject (e.g., reporting a compromised username/password combination) 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.
412c	**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.

This process is optional and may not be supported by all service providers.

418a	**Inputs**	Inaccessible Credential – The Subject is currently not able to use the Credential. This can be triggered by the Subject (e.g., reporting a compromised username/password combination) 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.
418b	**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.
418c	**Dependencies**	Credential Suspension

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.

425a	**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.
425b	**Outputs**	Updated issued Credential – A Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
425c	**Dependencies**	Credential Issuance, Authentication

3.2.8 Credential Revocation

The Credential Revocation process ensures that a Credential is permanently disabled or deleted. Once an 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.

433a	**Inputs**	Issued Credential – The Credential can be in any state other than Revoked (i.e., inaccessible or valid).
433b	**Outputs**	Revoked Credential – The Credential is permanently disabled or deleted. This is a permanent condition.
433c	**Dependencies**	Credential Issuance, Authentication

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 Authentication 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 Authentication Component has taken guidance from and is based in part on the following standards and guidance documents:

1. Government of Canada Guidance User Authentication User authentication guidance for information technology systems (ITSP.30.031 v3) - Canadian Centre for Cyber Security
2. Government of the United Kingdom. Cabinet Office and United Kingdom National Technical Authority on Information Assurance. Authentication and Credentials for

use with HMG Online Services (GPG-44). 2014. <Using authenticators to protect an online service >.

3. Government of the United States. United States Department of Commerce. National Institute of Standards and Technology. Digital Identity Guidelines (NIST Special Publication 800-63-3). 2017. <NIST Special Publication 800-63-3 >.
4. Government of the United States. United States Department of Commerce. National Institute of Standards and Technology. Digital Identity Guidelines: Enrollment and Identity Proofing Requirements (NIST Special Publication 800-63A). 2017. <NIST Special Publication 800-63B >
5. Government of the United States. United States Department of Commerce. National Institute of Standards and Technology. Digital Identity Guidelines: Authentication and Lifecycle Management (NIST Special Publication 800-63B). 2017. <NIST Special Publication 800-63A >
6. Government of the United States. United States Department of Commerce. National Institute of Standards and Technology. Digital Identity Guidelines: Federation and Assertions (NIST Special Publication 800-63C). 2017. <NIST Special Publication 800-63C >

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

- Government of Canada. Communications Security Establishment. Information Technology Security Guidance: IT Security Risk Management: A Lifecycle Approach (ITSG-33). 2012. IT security risk management: A lifecycle approach (ITSG-33) - Canadian Centre for Cyber Security
- Government of the United States. United States Department of Commerce. National Institute of Standards and Technology. Federal Information Processing Standards Publication 140-2 (Security Requirements for Cryptographic Modules). 2001. <Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules >
- Government of the United States. United States Department of Commerce. National Institute of Standards and Technology. Guide to Computer Security Log Management (Special Publication 800-92). 2006. <Guide to Computer Security Log Management >
- United States Department of Commerce. National Institute of Standards and Technology. Security and Privacy Controls for Federal Information Systems and Organizations (Special Publication 800-53 (Rev.4). <Access CPRT - Cybersecurity and Privacy Reference Tool | CSRC | CSRC >
- AXELOS. ITIL v3 (formerly the Information Technology Infrastructure Library). 2011. <ITIL | IT Service Management | Axelos >

5. Notes

- Source: Government of Canada. Treasury Board of Canada Secretariat.
- Guideline on Defining Authentication Requirements. <Guideline on Defining Authentication Requirements>The PCTF's definition of Authentication has been adopted from this Government of Canada publication.

- The Authentication Process is a dependency when the process is initiated by a user (e.g., a Subject or an administrator).

6. Appendix A: Authentication Use Cases

The following table outlines several authentication use cases to provide an overview of various implementations where authentication is required. These examples have been selected to highlight the differences between various authentication types, authentication factors and authenticators and includes considerations affecting a Level of Assurance determination.

	Examples (Authenticator Types)	**Authentication Factor**	**Authenticator**	**Authenticator Validation Data**	**Credential**	**Factors Influencing LOA Determinations**
501b	User Name and Password	Something you know	Subject's actual password	Hash of Subject's actual password	Data about the Subject associated with the Authenticator Validation Data (e.g., Subject's first name)	• Password strength policy • Strict adherence to the policy • See "Credential Maintenance" criteria in the Conformance Profile
501c	Verifiable Credentials in a mobile Digital Wallet	Something you have	A private key	Associated public key and certificate authority/issuer signature	Data about the Subject associated with the Authenticator Validation Data (e.g., Subject's first name)	• Key size • Signing algorithm • Local authentication type (e.g., user name and password, biometric) used to unlock the Digital Wallet See "Credential Maintenance" criteria in the Conformance Profile

501d	Biometric Authenticator	Something you are	Face	Geometric data (a sequence of measurements of face geometry such as the distance between the corner of the eye and tip of the nose)	Data about the Subject associated with the Authenticator Validation Data (e.g., Subject's first name)	• Algorithm used • Age of data • Confidence Thresholds • Liveness detections
501e	Federated Use Case	A Credential issued through a successful authentication process	OAuth/OIDC token	Validation of the associated cryptographic signature (e.g., Private JWT Key)	Data about the Subject associated with the Authenticator Validation Data (e.g., Subject's first name)	• Federation agreement • CSP assessments and auditability • Authentication context
501f	Mutual Transport Layer Security (mTLS)	Something you have	A private key	Associated public key and certificate authority/issuer signature	Data about the Subject associated with the Authenticator Validation Data (e.g., access control list entry)	• Key length • Key management policies and processes • Minimum supported versions

502 **Table 2. Authentication Use Cases**

503 7. Appendix B: Summary of Trusted Process
504 Conditions

505 Table 2 summarizes the input and output conditions of the PCTF Authentication
506 Component.
507

	Condition	Description
507a		
507b	No Credential	There is no Credential assigned to the Subject.

507c	Issued Credential	An Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
507d	Authenticated Credential	The Subject has successfully authenticated and proven control of the Credential at the specified Level of Assurance.
507e	Authentication Session	A persistent interaction between a Subject and an end-point.
507f	Inaccessible Credential	The Subject is currently not able to use the Credential. This can be triggered by the Subject (e.g., reporting a compromised username/password combination) 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.
507g	Revoked Credential	The Credential is permanently disabled or deleted. This is a permanent condition.

508
509 **Table 3. Authentication Component Conditions**

510 8. Appendix C: Summary of Trusted Process 511 Dependencies

512 Trusted Processes may need to rely on a condition that is the output of another Trusted
513 Process. This is referred to as a dependency. Table 3 summarizes the inputs, outputs,
514 and dependencies between the Trusted Processes of the PCTF Authentication
515 Component.
516

	Trusted Process	**Input Condition**	**Process Dependency**	**Output Condition**
516b	Authentication Credential Issuance	No Credential	-	Issued Credential
516c	Authentication	Issued Credential	Credential Issuance	Authenticated Credential
516d	Authenticated Session Initiation	Authenticated Credential	Authentication	Authenticated Session
516e	Authenticated Session Termination	Authenticated Session	Authenticated Session Initiation	No Authenticated Session
516f	Credential Suspension	Issued Credential	Credential Issuance	Inaccessible Credential
516g	Credential Recovery	Inaccessible Credential	Credential Suspension	Issued Credential

516h	Credential Maintenance	Issued Credential	Credential Issuance, Authentication	Issued Credential (updated)
516i	Credential Revocation	Inaccessible Credential	Credential Issuance, Authentication	Revoked Credential

517 **Table 4. Trusted Process Relationships**

518 # 9. Revision History

	Version	Date of Issue	Author(s)	Description
518b	.05	2018-01-24	TFEC	Initial working draft
518c	.06	2019-04-30	PCTF Editing Team	Formatting edits Updated PCTF Model Diagram
518d	.07	2019-10-21	TFEC and PCTF Editing Team	Revised content based on discussion draft comments
518e	1.0	2019-10-30	TFEC	Approved as Draft Recommendation V1.0
518f	1.1	N/A	PCTF Editing Team	Updates per comments received during draft recommendation review period
518g	1.0	2020-05-11	PCTF Editing Team	Approved as Final Recommendation V1.0
518h	1.1	2023-11-15	PCTF Authentication Design Team	Updates made to address feedback received through PCTF alpha testing and deferred comments from earlier iterations
518i	1.1	2023-12-01	PCTF Authentication Design Team	TFEC approves as Final Recommendation V1.1

519