PCTF Authentication Component Overview

Document Status: Final Recommendation V1.0

In accordance with the DIACC Operating Procedures, a Final Recommendation is a deliverable that represents the findings of a DIACC Expert Committee that have been approved by an Expert Committee and have been ratified by a DIACC Sustaining Member Ballot.

This document was developed by DIACC's Trust Framework Expert Committee with input from the public gathered and processed through an open peer review process. It is anticipated that the contents of this document will be reviewed and updated on a regular basis to address feedback related to operational implementation, advancements in technology, and changing legislation, regulations, and policy. Notification regarding changes to this document will be shared through electronic communications including email and social media. Notification will also be recorded on the Pan-Canadian Trust Framework Work Programme. Changes to this document that may affect certification and Trustmark status will be defined in the Pan-Canadian Trust Framework Assessment component.

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.

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 only in the context of unlocking access to another Authenticator. An example of such a scenario is someone using Apple's TouchID or FaceID to unlock an iPhone and subsequently access a one-time passcode or other locally stored and generated 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.

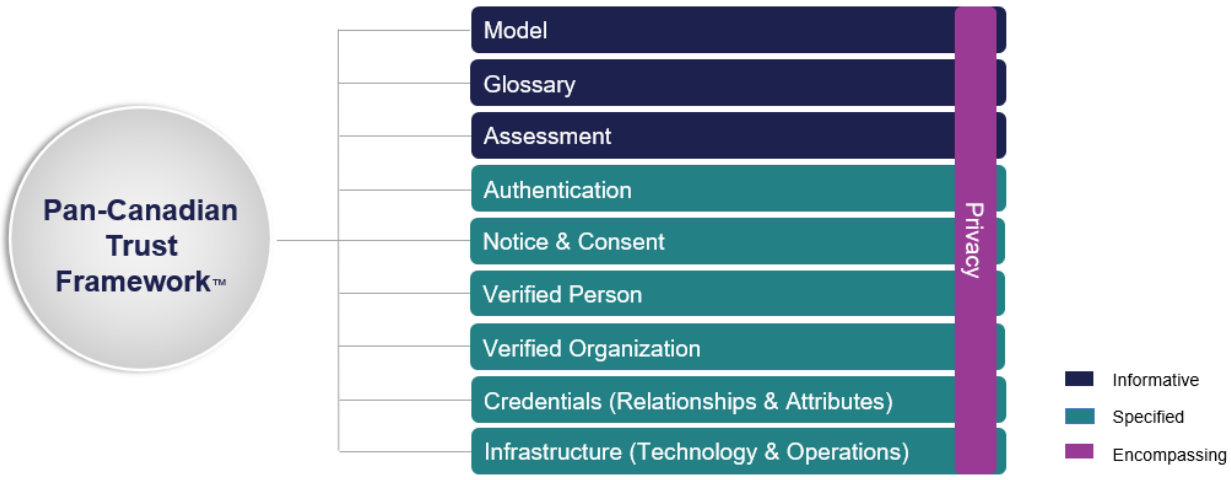

Figure 1. Components of the Pan-Canadian Trust Framework

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. 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 one-time-password (OTP) tokens – 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 an Authentication 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 001001101011111010000
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)

Authentication Credential

Data that uniquely binds Authenticator Validation Data to Identity data. For the purposes of this PCTF component, "Authentication 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 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.

Note

- Depending on the use case, different organizations may assume one or multiple roles. For example, Authentication 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 Authentication Credentials:

1. Authentication Credential Issuance
2. Authentication Credential Suspension
3. Authentication Credential Recovery
4. Authentication Credential Maintenance
5. Authentication 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 Authentication 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. The requirements of each LOA are cumulative – successively higher LOAs require that the requirements for lower LOAs have been met as well.**

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

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 1. Levels of Assurance

Note

- 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 a qualifier. For example, a Relying Party in the health care sector may specify in a PCTF Profile a requirement for an LOA3 Authentication 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 Authentication Credential Issuance process to transform a “No Authentication Credential” input condition to an “Issued Authentication 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. Authentication Credential Issuance
2. Authentication
3. Authenticated Session Initiation
4. Authenticated Session Termination
5. Authentication Credential Suspension
6. Authentication Credential Recovery
7. Authentication Credential Maintenance
8. Authentication 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.

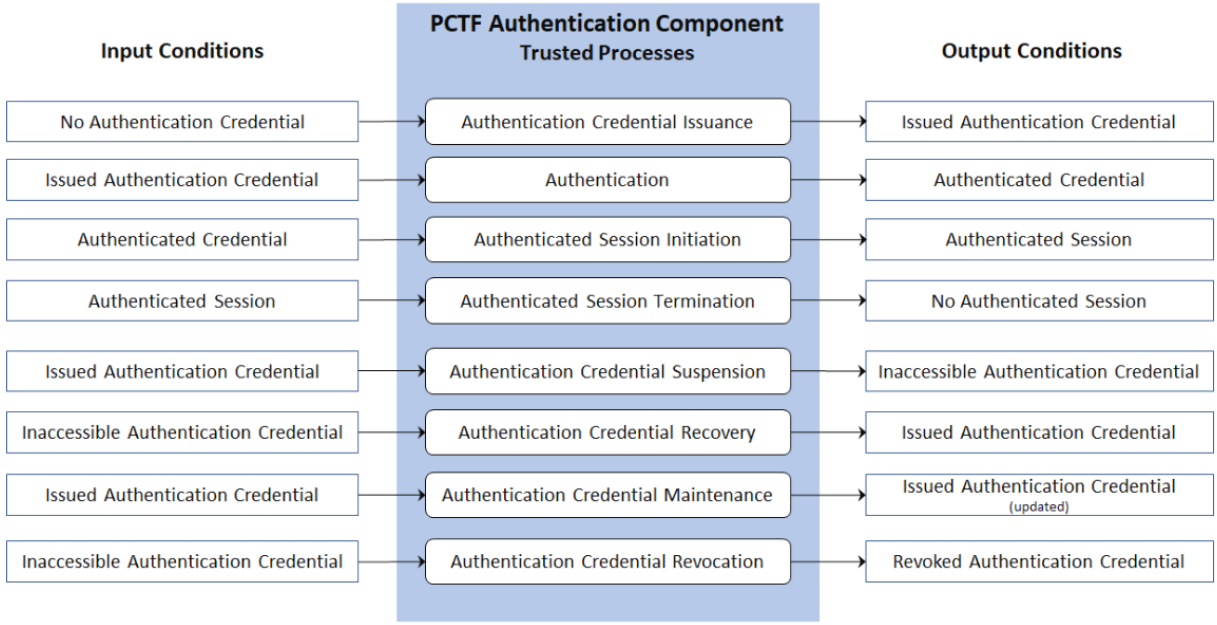

Figure 2. Authentication Component Conceptual Overview

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 Authentication Credential Issuance

Authentication Credential Issuance is an enrolment process during which an Authentication Credential is issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject. An Authentication Credential includes one or more identifiers which may be pseudonymous and may contain attributes verified by the Authentication 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.

Inputs	No Authentication Credential – There is no Authentication Credential assigned to the Subject.
Outputs	Issued Authentication Credential – An Authentication Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
Dependencies	

3.2.2 Authentication

Authentication is the process of establishing truth or genuineness to generate an assurance.[1] 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.

Inputs	Issued Authentication Credential – An Authentication 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 Authentication Credential at the specified LOA.
Dependencies	Authentication Credential issuance

3.2.3 Authenticated Session Initiation

At some point during a Session a sub-session may be initiated to Authenticate a Subject. This Authenticated Session Initiation must begin with an Authenticated Credential. The output of the Authenticated Session Initiation is an Authenticated Session.

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.

Inputs	Authenticated Credential – The Subject has successfully authenticated and proven control of the Authentication Credential at the specified LOA.
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.
Dependencies	Authentication

3.2.4 Authenticated Session Termination

The Authenticated Session Termination process is required when Authenticated 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'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.
Outputs	No Authenticated Session

Dependencies	Authenticated Session Initiation

3.2.5 Authentication Credential Suspension

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

Inputs	Issued Authentication Credential – An Authentication Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
Outputs	Inaccessible Authentication 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.
Dependencies	Authentication Credential Issuance

3.2.6 Authentication Credential Recovery

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

Inputs	Inaccessible Authentication Credential – The Subject is currently not able to use the Authentication 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 Authentication Credential.
Outputs	Issued Authentication Credential – An Authentication Credential has been issued, bound to a single Subject, and bound to one or more appropriate Authenticators controlled by the Subject.
Dependencies	Authentication Credential Suspension

3.2.7 Authentication Credential Maintenance

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

3.2.8 Authentication Credential Revocation

The Authentication Credential Revocation process ensures that an Authentication Credential is permanently disabled or deleted. Once an Authentication Credential is revoked, it can no longer be used. The system will actively prevent further Trusted Processes from occurring in relation to this Authentication Credential. The process can be initiated by a User, system administrator, or automatically by the system. Note that a new Authentication Credential can be issued for the same Subject. Re-issue equates to revoking an Authentication Credential and issuing a new Authentication Credential for the same Subject.

Inputs	Inaccessible Authentication Credential – The Subject is currently not able to use the Authentication Credential.
Outputs	Revoked Authentication Credential – The Authentication Credential is permanently disabled or deleted. This is a permanent condition.
Dependencies	Authentication 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 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. Communications Security Establishment. *Information Technology Security Guidance for Practitioners: User Authentication Guidance for*

Information Technology Systems (ITSP.30.031 V3). 2018. <https://www.cse-cst.gc.ca/en/publication/itsp.30.031v3>.

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. <https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services>.
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. <https://pages.nist.gov/800-63-3/sp800-63-3.html>.
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. <https://pages.nist.gov/800-63-3/sp800-63b.html>
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. <https://pages.nist.gov/800-63-3/sp800-63a.html>
6. Government of the United States. United States Department of Commerce. National Institute of Standards and Technology. D*igital Identity Guidelines: Federation and Assertions (NIST Special Publication 800-63C).* 2017. <https://pages.nist.gov/800-63-3/sp800-63c.html>

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

1. Government of Canada. Communications Security Establishment. *Information Technology Security Guidance: IT Security Risk Management: A Lifecycle Approach (ITSG-33)*. 2012. < https://cyber.gc.ca/en/guidance/overview-itsg-33>
2. Government of Canada. Treasury Board Secretariat. *Password Guidance*. 2020. < https://www.canada.ca/en/government/system/digital-government/online-security-privacy/password-guidance.html>
3. 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. <https://csrc.nist.gov/publications/detail/fips/140/2/final>
4. 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. < https://www.nist.gov/publications/guide-computer-security-log-management>
5. 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)*. < https://nvd.nist.gov/800-53/Rev4/control/IA-5>
6. AXELOS. *ITIL v3 (formerly the Information Technology Infrastructure Library).* 2011. <https://www.axelos.com/best-practice-solutions/itil>

5 Notes

1. Source: Government of Canada. Treasury Board of Canada Secretariat. *Guideline on Defining Authentication Requirements.* <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262&section=html> The PCTF's definition of Authentication has been adopted from this Government of Canada publication.
2. 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 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 Authentication 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

7 Appendix B: Summary of Trusted Process Conditions

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

Condition	Description
No Authentication Credential	There is no Authentication Credential assigned to the Subject.
Issued Authentication Credential	An Authentication 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 Authentication Credential at the specified Level of Assurance.
Authentication Session	A persistent interaction between a Subject and an end-point.
Inaccessible Authentication Credential	The Subject is currently not able to use the Authentication 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 Authentication Credential.
Revoked Authentication Credential	The Authentication Credential is permanently disabled or deleted. This is a permanent condition.

Table 2. Authentication Component Conditions

8 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 Authentication Component.

Trusted Process	Input Condition	Process Dependency	Output Condition

Authentication Credential Issuance	No Authentication Credential	-	Issued Authentication Credential
Authentication	Issued Authentication Credential	Authentication Credential Issuance	Authenticated Credential
Authenticated Session Initiation	Authenticated Credential	Authentication	Authenticated Session
Authenticated Session Termination	Authenticated Session	Authenticated Session Initiation	No Authenticated Session
Authentication Credential Suspension	Issued Authentication Credential	Authentication Credential Issuance	Inaccessible Authentication Credential
Authentication Credential Recovery	Inaccessible Authentication Credential	Authentication Credential Suspension	Issued Authentication Credential
Authentication Credential Maintenance	Issued Authentication Credential	Authentication Credential Issuance, Authentication [2]	Issued Authentication Credential (updated)
Authentication Credential Revocation	Inaccessible Authentication Credential	Authentication Credential Issuance, Authentication [2]	Revoked Authentication Credential

Table 3. Trusted Process Relationships

9 Revision History

Version	Date of Issue	Author(s)	Description
.05	2018-01-24	TFEC	Initial working draft
.06	2019-04-30	PCTF Editing Team	Formatting edits Updated PCTF Model Diagram
.07	2019-10-21	TFEC and PCTF Editing Team	Revised content based on discussion draft comments.
1.0	2019-10-30	TFEC	Approved as Draft Recommendation V1.0
1.1	N/A	PCTF Editing Team	Updates per comments received during draft recommendation review period.
1.0	2020-05-11	PCTF Editing Team	Final Recommendation V1.0