PCTF Authentication

Document Status: Final Recommendation V1.2

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 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.

Table of contents

1. Introduction to the PCTF Authentication Component

Content herein concerns itself with the domain specific topic for this Pan-Canadian Trust Framework (PCTF) component. The overview section provides information related to and necessary for consistent interpretation of the included conformance criteria. For a general introduction to the PCTF, please see the PCTF Overview that describes the background, purpose, scope, principles, and objectives of the framework.

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.

- When combined with considerations from the PCTF Wallet Component, participants may have an enhanced user experience through the reuse of credentials across multiple Relying Parties.

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 would be to employ a biometric solution that works across channels via facial, fingerprint or voice recognition (something you are) in addition to another authentication method such as control and possession of a mobile device (something you have).

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 Pan-Canadian Trust Framework.

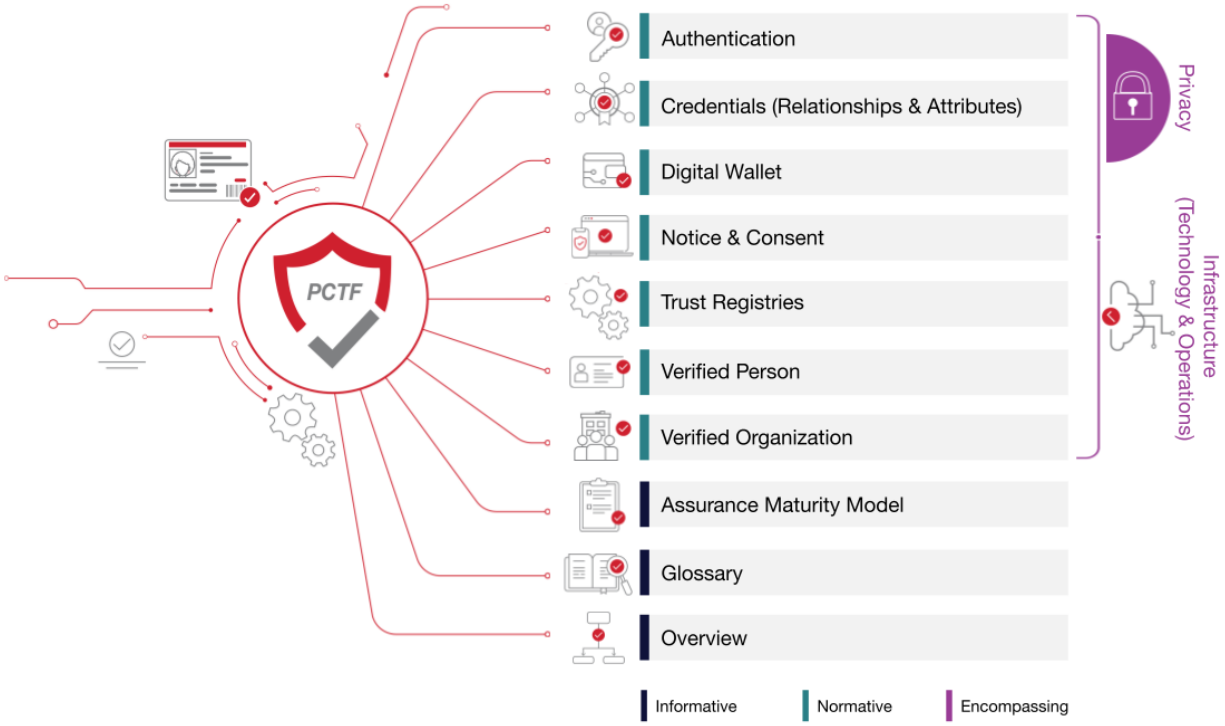

Figure 1. Components of the Pan-Canadian Trust Framework

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
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

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.

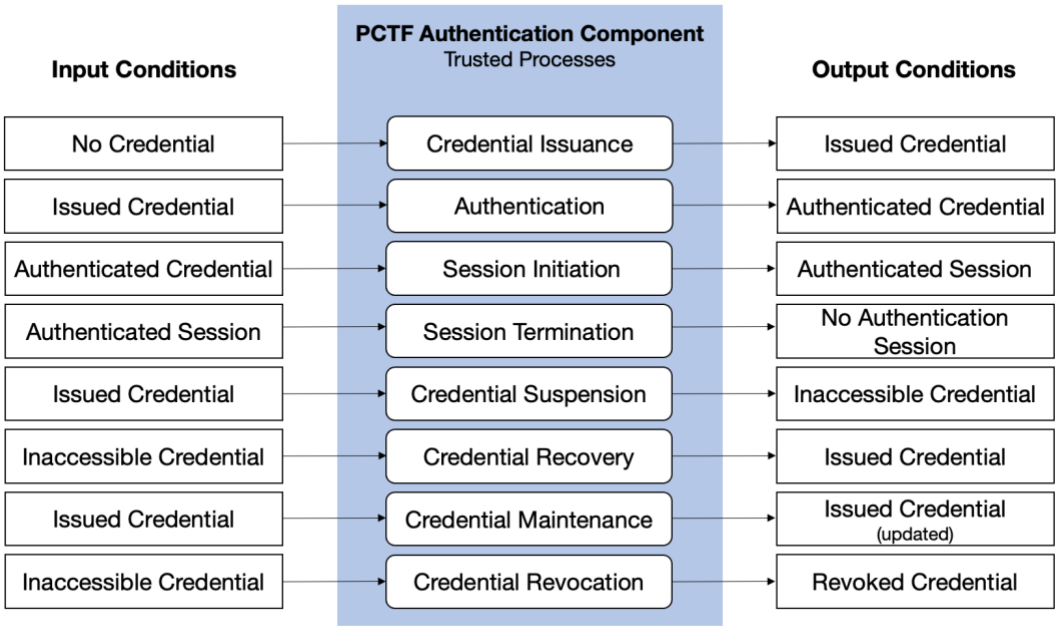

Figure 2. Authentication Component Conceptual Overview

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

Notes:

- 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.

Inputs	No Credential – There is no Credential assigned to the Subject.
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	

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.

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	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

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.

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'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 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.

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 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.

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., 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	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.

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.

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 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.

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	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.
Dependencies	Credential Issuance, Authentication

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

4. Introduction to the PCTF Authentication Component Conformance Criteria

The Conformance Criteria specified herein can be used to assure the on-going integrity of login and authentication processes such that they 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.

4.1 About PCTF Conformance Criteria

The PCTF promotes trust through a set of auditable business and technical requirements for various 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. Conformance Criteria are the requirements and specifications that comprise a standard for these processes. They can be used to assess the integrity of a process. 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 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. Conformance criteria are therefore central to the trust framework because they specify the requirements that ensure process integrity.

Note: PCTF Conformance Criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy and regulations in their jurisdiction.

5. Authentication Conventions

Each PCTF component includes conventions that ensure consistent use and interpretation of terms and concepts appearing in the component. These conventions include definitions and descriptions of the following items that are referred to in this conformance profile:

- Key terms and concepts
- Abbreviation and acronyms

- Roles
- Levels of Assurance
- Trusted Processes and associated conditions

Notes:

- Conventions may vary between PCTF components. Readers are encouraged to review the conventions for each PCTF component they are reading.
- Defined Terms – For purposes of this conformance profile, terms and definitions listed in both the PCTF Authentication Component Overview and the PCTF Glossary apply. Key terms and concepts described and defined in this section, or the PCTF Authentication Component Overview, or 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.
- All references to the term ‘credential within this document refer to an 'Authentication Credential’. The shorter version is used herein to improve readability.

5.1 Conformance Criteria Keywords

Throughout this document the following terms indicate the precedence and/or general rigidity of the Conformance Criteria and are to be interpreted as noted below.

- **MUST** means that the requirement is absolute as part of the Conformance Criteria.
- **MUST NOT** means that the requirement is an absolute prohibition of the Conformance Criteria.
- **SHOULD** means that while there may exist valid reasons in particular circumstances to ignore the requirement, the full implications must be understood and carefully weighed before choosing to not adhere to the Conformance Criteria or choosing a different option as specified by the Conformance Criteria.
- **SHOULD NOT** means that a valid exception reason may exist in particular circumstances when the requirement is acceptable or even useful, however, the full implications should be understood and the case carefully weighed before choosing to not conform to the requirement as described.
- **MAY** means that the requirement is discretionary but recommended.

Note: The above listed keywords appear in **bold** typeface and ALL CAPS throughout this conformance profile.

5.2 Authentication Risks

Type of Risk	Threat category	Threat scenario / Vulnerability	Additional info	Threat Agent	Impact	Proposed safeguards (e.g., input to conformance requirements)
Information security → harm to Holder, harm to Relying Parties	Product or service quality risk	Product or service contains software vulnerabilities	• Accidental or malicious intent	• Hacker/attacker • Unintended consequences of software flaws	Harm to ecosystem participants: • Trust in ecosystem • Reputational risk of ecosystem as a whole Harm to Holder: • Identity theft • Financial harm • Loss of privilege/access/use • Reputational harm Harm to Relying Parties: • Financial harm • Loss of privilege/access/use • Reputational harm • Privacy harm	• Product or service undergoes a certification process, and as appropriate, re-certification process, and has a Trustmark proving implementer follows standard industry practice product development processes throughout entire lifecycle. • Considerations for supply chain integrity validation, security in the SDLC, 3rd party security assessments, vulnerability management process
Information security lifecycle management → user inconvenience	Product or service quality risk	Product or service is no longer supported and is obsolete	• Unpatched flaws • Lack of interoperability/	• Malicious actors targeting unpatched software • Unusable	• Holder is unable to perform required transactions • Credential or access	• Product and/or service should be updated or replaced with a compatible and/or more secure replacement and a patch

			utility	software (incompatible)	compromised	management regimen should be maintained
Information security → harm to Holder	Product or service provider integrity/supply chain risk	Malicious actors provide product or service with intent to harm customers	• Malicious actors provide product or service. This may resemble a well-known product or service.	• Malicious product or service provider	• Impersonate Holder • Privacy harm to Holder • Reputation harm to Holder	• Customer properly assesses product or service providers; Customers may rely on certifications and/or Trustmarks
Information security lifecycle management → user inconvenience.	product or service quality risk	Product or service does not implement, or conform to, industry standards	• Product or service is unable to interoperate with applications or other systems	• Product or service provider	• Denial of Service to the Customer • Holder is unable to perform required transactions • Issuer unable to issue • Verifier not able to verify	• Product or service implements industry standards as proved by an appropriate certification program or Trustmark • Verify interoperability with recognized industry standards such as X.509, TOTP, SAML, OIDC family, W3C Verifiable Credentials, etc.
Information security lifecycle management → user inconvenience.	Product or service quality risk	Product or service has inadequate technical security controls to mitigate denial-of-service conditions	• Implementation of product/service was not appropriately monitored.	• Malicious actor(s) (remote)	• System is subject to Denial-Of-Service (DOS) attacks, rendering the service completely or partially unavailable to users.	• Product or service provider undergoes a certification process and has a Trustmark verifying conformance to standard industry practices. • Implement anti-DOS measures such as selective geo-fencing, subscription to DDOS mitigation services

						from cloud providers, etc.
Information security → harm to Holder.	Product or service quality risk	Product or service has inadequate technical security controls or management practices	• Implementation of product/service was not appropriately monitored	• Hacker	• System is easily compromised, which could expose data, or allow a sophisticated attacker to issue unauthorized Credentials or to bypass access controls	• Product or service provider undergoes a certification process and has a Trustmark proving conformance to standard industry practices. • Considerations for supply chain integrity validation, security in the SDLC, 3rd party security assessments, vulnerability management process.
Information security: key management → harm to Subjects	Unauthorized data access risk	Operating environment does not support required security functions for specific/target LOA(s)	• Standard industry key management tools and processes are not used, or not used effectively	• Malicious actor (local or remote)	• Compromised keys/privacy breach/identity theft/unauthorized data access	• Product or service provider explicitly supports adequate/evaluated key management capability • **Notes:** ○ This includes key management functions & high-impact security functions managed on product or service infrastructure and/or end-user equipment ○ "Adequate" (FIPS for hardware, NIST for software) will depend on LOA
Information security: key management	Backup and recovery risks/key	Product or service has inadequate	• Malicious actor steals secret	• Malicious actor	• Compromised keys/unauthorized data	• Backup and recovery processes to be defined for

security → harm to Subjects	management risks	backup and recovery controls	keys using backup/recovery mechanism	(local or remote)	access/privacy breach/identity theft	the corresponding LOA and assessed as part of the certification process • Backups must have same LOA protections as the original or "live service" protections
Information security: key management security → harm to Subjects	Infrastructure, software or device-related security risks/key management risks	Product or service does not support required security functions for specific/target LOA(s).	• Product or services software does not have adequate key management protections. • Malicious actor steals secret keys (e.g., steals key from memory, cracks white box crypto, power analysis)	• Malicious actor (local or remote)	• Compromised keys/unauthorized data access/privacy breach/identity theft	• Product or service uses adequate/evaluated key management software and/or hardware with non-exportable keys • **Note:** "adequate" (NIST for software) will depend on LOA
Information security: data analytics → harm to Subjects	Data analytics in the Product or Service	Product or service allows (or does not properly disallow) sharing of sensitive information. (e.g., Sensitive information being passed in data analytics collection)	• Unintentional or intentional	• Malicious actor or insufficiently trained workforce	• Sensitive data leakage in analytics data • Privacy breach/identity theft	• If sensitive data required in analytics, ensure anonymized, or tokenized and encrypted before being sent - including before saved to local storage in offline modes and backups • Trust mark to ensure privacy risk assessment is completed when adding/modifying data

						analytics - where assessment includes risk of unintended use of analytics data • Trust mark to ensure access control requirements on access to analytics data • Training of workforce with standard data privacy practices
Information security: environment security → harm to Subjects	Insider security risks	Product or service provider personnel are compromised	• Social Engineering	• Unauthorized data access/Non-Subject Access	• Privacy breach/identity theft	• Product or service provider to check for known vulnerabilities on launch, notifies Subjects/Customers of specific vulnerabilities and required corrective actions prior to product or service use • LOA driven requirements
Information security: environment security → harm to Subject	Insider security risks	Credential holder is compromised	• Social Engineering	• Unauthorized data access/Non-Subject Access	• Privacy breach/identity theft	• Product or service provider to check for known vulnerabilities on launch, notifies Subjects/customers of specific vulnerabilities and required corrective actions prior to product or service use • LOA driven requirements
Information security: Binding and authentication	Unauthorized use of the product or	Authenticator compromise	• When users share devices, authenticators	• Hackers • Acquaintances	• Assertions are made on the behalf of the user	• Include specific language in the EULA to ensure authorized users understand

→ harm to Subject	service		without proper access controls could allow others to share the information of the authorized holder without their consent	• Family Members	without their consent	their responsibility. • Provide authentication experiences that do not depend exclusively on possession and control of a single device. • Apply additional Anti-Spoofing and Liveness Detection Techniques (ISO-30107)
Privacy → user tracking	User tracking	Identifying information correlation without notice or consent	• Product or service uses common identifiers across multiple verifiers	• Invasion of privacy	• Linking of identifiers across Verifiers • User tracking • Data aggregation	• Product or service uses standard unique identifiers technologies such as: ○ URI (e.g., various DID methods) ○ UUID ○ GUID
Privacy → oversharing	Oversharing	Product or service does not support data minimization	• Subject provides more information to Verifier than appropriate	• Rogue Verifier targeting user of specific Product or Service that does not offer data minimization capabilities • Unintended Verifier that receives more information than it asked for/needs	• Holder provides more information to Verifier than appropriate • Privacy breach/identity theft • Verifier privacy regulation non-compliance for receipt of data it did not have a business need for • Inability for government Verifier use as government may not have authority to receive additional information not asked for	• Product or service to support data minimization capabilities (e.g., selective disclosure, ZKP)

Privacy → oversharing	Oversharing	End-user choice of Credential and/or claims may result in disclosure of information not strictly required	• Incomplete, unclear, or ambiguous notice	• Product or Service provider (introduces threat) - quality issue • Rogue Verifier targeting user of specific Products or Services that do not offer proper notice	• Holder provides more information to Verifier than they would have otherwise agreed to; Decisions being made by Verifier on that information could have negative impact to that user • Holder not able to accurately assess risk of information disclosure	• Product or service effectively discloses information to be shared to Holder and allows Holder to control • Data that may not be 'understandable' (i.e., encoded data) should be described in plain language
Privacy → oversharing	Oversharing	Product or service collects more claims than are strictly required	• Subject provides more information to Verifier than appropriate. Incomplete, unclear, or ambiguous notice	• Product or service provider puts additional information at risk	• Holder not able to accurately assess risk of information disclosure	• Product or service effectively limits information it collects • Product or service provides full and complete notice to the Holder
Compliance → privacy	Privacy	Product or service does not conform to PCTF Privacy component	N/A	N/A	• Privacy non-compliance	• Trustmark to ensure PCTF Privacy Component compliance as part of product or service certification
Accessibility	User experience	Product or service does not confirm to industry accessibility standards	N/A	N/A	• Holder is unable to use product or service due to disabilities; Subject vulnerable population to alternate processes or tools that may carry	• Product or service implements industry standard accessibility capabilities

					different risks to privacy • Abandonment; reputational risk • Lack of service; Over-sharing of data	
Usability	User experience	Product or service instructions are not clear	• Product or service instructions are not clear to the Holder • Notice is unclear or ambiguous • Poor user experience	N/A	• Holder uses product or service in an unintended way that results in harm to the Holder • Release of PII to unintended recipient (accidental privacy breach; phishing)	• Product or service uses plain language and has consistent look and feel • Robust product or service design: Prevent access to, or sharing from, without validating the entities information is being exchanged with
Information security: data registry security → harm to Subject	Governance	Product or service relies on (trusts) a credential authority that is not (or no longer) appropriate	• Product or Service trusts public key of malicious actor	• Malicious actor that establishes a rogue data registry or registry entry	• Users make unintentional/uninformed sharing decisions • Privacy breach/identity theft	• Product or service authenticates Data Registry as Trusted; where, authentication implies a capability to ensure “is legitimate” or “is suitable for the defined purpose”
Information security: channel compromise → risks to Subject	Missing authentication	Authentication channel is insecure or compromised. (i.e., Attacker in the Middle) Insecure session management or	N/A	• Malicious 3rd party	• Unauthorized data access, privacy • Identity theft • Unauthorized actions	• Product or service implements appropriate controls to meet the selected LoA • Product or service has the controls it has implemented audited and/or actively tested for effectiveness

		session hijacking				
Information security: stored information compromise	Compromised keys	Credential Storage: Insecure storage of Credentials can lead to unauthorized access if the stored data is compromised	• Secure backups • Secure key storage	• Malicious 3rd party	• Privacy breach • Identity theft • Authorized access to data and/or activity	• Product or service implements appropriate controls to meet the selected LOA • Product or service has the controls it has implemented audited and/or actively tested for effectiveness

6. Authentication Component Conformance Criteria

The following sections define Conformance Criteria that are essential requirements for the Trusted Processes of the Authentication Component. The Authentication Trusted Process are:

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

Conformance criteria are categorized by Trusted Process and profiled in terms of Levels of Assurance. Conformance Criteria are grouped by topic within each category. For ease of reference, a specific conformance criterion may be referred to by its category and reference number. Example: "**BASE-1**" refers to "Baseline Conformance Criteria reference No. 1".

Notes:

- Baseline Conformance Criteria are also included as part of this conformance profile.
- Conformance Criteria specified in other PCTF components of may also be applicable to Authentication Trusted Processes under certain circumstances.
- Notification Conformance Criteria specified in this conformance profile represent only those notifications specific to processes in the context of the PCTF Authentication Component. See the PCTF Notice and Consent Component for additional notification-related Conformance Criteria.
- LOA 4 is out of scope for this version. Reference is retained as a placeholder for future development.
- Further guidance on policy and operational controls supporting the Authentication Conformance Profile can be found in the PCTF Infrastructure (Technology & Operations) Conformance Profile.

Reference	Conformance Criteria	Level of Assurance (LOA)			
BASE	**Baseline**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
EVENT LOGGING					
1	Credential use events **MAY** be logged and retained for a predefined period of time as evidence.	X			
2	Credential use events **SHOULD** be logged and retained for a predefined period of time as evidence.		X		
3	Credential use events **MUST** be logged and retained for a predefined period of time as evidence.			X	
4	Credential management and use event logs **MUST** be: • Traceable back to a specific Credential and include the result and date and time of the logged event. • Protected by access controls to limit access only to those who require it (see NIST Special Publication 800-92 for recommendations concerning computer security log management).		X	X	
5	Credential management and use event logs **MUST** have a tamper-detection mechanism to detect unauthorized modifications.		X	X	
6	Personal information and authenticator secrets (e.g., passwords, OTP values, security questions, security answers) **MUST NOT** be logged within the service.	X	X	X	
INFORMATION SECURITY					
7	The Credential Service Provider/Authentication Service Provider **MAY** ensure i) the integrity, ii) the confidentiality, and iii) the availability of the service by adhering to a set of information security guidelines and controls (e.g., CSEC ITSG-33) that support these efforts.	X			
8	The Credential Service Provider/Authentication Service Provider **MUST** nsure the integrity, the confidentiality, and the availability of the service by adhering to a set of information security guidelines and controls (e.g., CSEC ITSG-33) that support these efforts.		X	X	

9	The Credential Service Provider/Authentication Service Provider **MUST** have an independently audited control report to demonstrate adherence to a set of information security guidelines and controls.			X	
IT SERVICE MANAGEMENT					
10	The Credential Service Provider/Authentication Service Provider **SHOULD** have a documented service management practice for all aspects of the service it provides related to PCTF Authentication Component Trusted Processes.	X			
11	The Credential Service Provider/Authentication Service Provider **MUST:** Establish and maintain a documented service management practice for all aspects of the service it provides related to PCTF Authentication Component Trusted Processes.		X		
12	The Credential Service Provider/Authentication Service Provider **MUST**: • Establish and maintain a documented service management practice for all aspects of the service it provides related to PCTF Authentication Component Trusted Processes. • Have a documented and independently audited service management practice for all relevant aspects of the service it provides related to PCTF Authentication Component Trusted Processes.			X	
13	The Credential Service Provider/Authentication Service Provider **SHOULD** adhere to an industry standard service management framework (e.g., ITIL).	X	X		
14	The Credential Service Provider/Authentication Service Provider **MUST** adhere to an industry standard service management framework (e.g., ITIL).			X	
MONITORING					
15	The Credential Service Provider/Authentication Service Provider **SHOULD** have controls to detect misuse or compromise of the Credential.	X			

16	The Credential Service Provider/Authentication Service Provider **MUST** have controls to detect misuse or compromise of the Credential.		X	X	
17	The Credential Service Provider **SHOULD** initiate the Credential Suspension process, the Credential Maintenance process, or the Credential Revocation process when it finds actionable indications of Credential misuse or compromise.	X			
18	The Credential Service Provider **MUST** initiate the Credential Suspension process, the Credential Maintenance process, or the Credential Revocation process when it finds actionable indications of Credential misuse or compromise.		X	X	
PRIVACY					
19	The Credential Service Provider/Authentication Service Provider **SHOULD** adhere to the privacy risk management practices of the PCTF Privacy Component and any relevant PCTF Profiles applicable to the digital ID service.	X			
20	The Credential Service Provider/Authentication Service Provider **MUST** adhere to the privacy risk management practices of the PCTF Privacy Component and any PCTF Profiles applicable to the digital ID service.		X	X	
21	The Credential Service Provider/Authentication Service Provider **MUST** adhere to privacy risk management practices that are accepted by and applicable to all parties participating in the digital ID service.		X	X	
NOTIFICATIONS					
22	The Credential Service Provider **MAY** notify the Subject without delay (e.g., immediate notification by email, text, or as prescribed by a CSP's policy) of any changes to individual Credential information (e.g., password update, adding or removing Authenticators).	X			
23	The Credential Service Provider **MUST** notify the Subject without delay (e.g., immediate notification by email, text, or as prescribed by a CSP's policy) of any changes to individual Credential information (e.g., password update, adding or removing authenticators).		X	X	
CDIS	**Credential Issuance**	**LOA1**	**LOA2**	**LOA3**	**LOA4**

BINDING SUBJECT					
1	The Credential Service Provider **SHOULD** enforce that the Credential is only bound to one Subject.	X			
2	The Credential Service Provider **MUST** enforce that the Credential is only bound to one Subject.		X	X	
3	The Credential Service Provider **MAY** document, or have a documented process for demonstrating, the Level of Assurance of the Subject's identity when the Credential was issued.	X			
4	The Credential Service Provider **MUST** document, or have a documented process for demonstrating, the Level of Assurance of the Subject's identity when the Credential was issued.		X	X	
5	The Credential Service Provider **MUST** make information available to Authentication Service Providers to verify the current state of any Credentials it has issued unless privacy constraints prohibit the sharing of this information (e.g., if a credential is an "Inaccessible Credential" or a "Revoked Credential", the minimum necessary status information must be available to Authentication Service Providers if allowable.)	X	X	X	
BINDING AUTHENTICATORS					
6	The Credential Service Provider **MAY** provide the ability to bind an Authenticator provided by the Subject to the Credential.	X	X	X	
7	The Credential Service Provider **MUST** bind at least one Authenticator to the Credential. (e.g., password, Q&A, or OTP).	X			
8	The Credential Service Provider **MUST** bind two or more Authenticators to the Credential. (e.g., password, Q&A, or OTP).		X	X	
9	At least two different Authenticators **SHOULD** be bound to the Credential such that recovery of one authenticator (e.g., from loss or theft) is possible using another Authenticator (e.g., an authenticator account could be recovered with a one-time-use recovery code).		X		

10	At least two different Authenticators **MUST** be bound to the Credential such that recovery of the primary Authenticator (e.g., from loss or theft) is possible using another Authenticator (e.g., an authenticator account could be recovered with a one-time-use recovery code).			X	
11	Additional Authenticators, which could be used for recovery purposes, **MUST** be the same or higher LOA as an Authenticator to be recovered.		X	X	
12	The Credential Service Provider **MAY** document, or have a documented process for, demonstrating the Level of Assurance of the Subject's identity when the Credential was recovered.	X			
13	The Credential Service Provider **MUST** document, or have a documented process for, demonstrating the Level of Assurance of the Subject's identity when the Credential was recovered.		X	X	
AUTHENTICATOR CREATION					
14	When the Authenticator is created (e.g., hardware OTP device OR software OTP), the creator **MUST** have an auditable quality management system and control processes		X		
15	When the Authenticator is created (e.g., hardware OTP device OR software OTP), the creator **MUST** have an Independently auditable quality management system and control processes.			X	
16	When the Authenticator uses information embedded by a manufacturer (e.g., hardware OTP device OR software OTP), the Credential Service Provider **MUST** ensure that there is an auditable security management control process that protects that information from compromise beginning from manufacture time through delivery to the Credential Service Provider.		X		
17	When the Authenticator uses information embedded by a manufacturer (e.g., hardware OTP device OR software OTP), the Credential Service Provider **MUST** ensure that there is an Independently Audited security management control process that protects that information from compromise beginning from manufacture time through delivery to the Credential Service Provider.			X	

CREDENTIAL STORAGE					
18	The Credential Service Provider/Authentication Service Provider **MUST** enforce access controls to prevent unauthorized access to Credential information.	X	X	X	
19	Any secrets bound to the Credential **MUST** be either stored as a salted hash or stored encrypted.		X	X	
20	Any Credential attributes containing personal information that are stored within the service **MUST** be secured (e.g., encrypted and/or hashed).	X	X	X	
21	Backups of Credential information **MUST** be encrypted prior to being transferred to long term storage and **MUST** remain encrypted while in storage.		X	X	
22	Cryptographic modules **MUST** meet an industry recognized Validation standard (e.g. FIPS 140-3 or comparable).		X	X	
AUTH	**Authentication**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
AUTHENTICATORS					
1	The Authentication Service Provider **MUST** require at least a single Authenticator of the following types: • Something the Subject knows; • Something the Subject has; or, • Something the Subject is or does.	X	X		
2	If only a single Authenticator is required, that Authenticator **MUST** be of an Authenticator Type that is either "something the Subject knows" or "something the Subject has". The "something the Subject is or does" Authenticator Type **MUST** only be used as secondary Authenticators.		X		
3	The Authentication Service Provider **MUST** require at least two different Authenticators that: • Provide different Authentication Factors; and • Are not susceptible to the same threat vectors.			X	

4	Of the different Authenticators required by the Authentication Service Provider by the **AUTH** criteria: • One of the Authenticators **MUST** be of the type "something the Subject has"; and • The other Authenticator(s) **MAY** be an Authenticator Type that is either "something the Subject knows" or "something the Subject is or does".			X	
5	The Authentication Service Provider **MUST** consult any information made available by the Credential Service Provider to determine the current state of a Credential.	X	X	X	
6	A biometric **SHOULD NOT** be used unless it is demonstrably necessary and is the best mechanism to meet a specific authentication need considering the commensurate potential loss of privacy.	X	X	X	
AUTHENTICATOR TYPE					
7	Any Authenticator Type **MAY** be used.	X			
8	The Authentication Service Provider **MUST** use an industry standard or best practice for authentication (e.g., standards and practices developed and approved by Kantara, W3C, IETF or FIDO Alliance).		X	X	
9	The Authentication Service Provider **MUST** use Authenticator Types that are resistant to the threats listed in the **THREAT MITIGATION** criteria for LOA3.			X	
THREAT MITIGATION					
10	The Authentication Service Provider **MUST** have effective control processes to prevent, detect and recover from at least the following types of attacks: • Authenticator secret guessing; and • Replay attacks. This **MAY** be included in the scope of the guidelines described in the **BASE** criteria.	X			

11	The Authentication Service Provider **MUST** have effective control processes to prevent, detect and recover from at least the following types of attacks: • Authenticator secret guessing; • Replay; • Eavesdropping; and • Session hijacking. This **MUST** be included in the scope of the controls described in the **BASE** criteria.		X		
12	The Authentication Service Provider **MUST** have effective control processes to prevent, detect and recover from at least the following types of attacks: • Authenticator secret guessing; • Replay; • Eavesdropping; • Session hijacking; • Impersonation/phishing; and • Man-in-the-middle attacks (e.g., using mutually authenticated TLS). This **MUST** be included in the scope of the independent audit process required by the **BASE** criteria.			X	
ADAPTIVE RISK					
13	The Authentication Service Provider **MAY** provide the ability to perform Adaptive Risk Authentication.	X			
14	The Authentication Service Provider **SHOULD** provide the ability to perform Adaptive Risk Authentication.		X		
15	The Authentication Service Provider **MUST** detect and mitigate interactions that represent high risk, based on information from the context of the authentication (such as transactions that originate from an unexpected location or channel for a Subject, or that indicate an unexpected hardware or software configuration) -or- The Authentication Service Provider **MUST** treat every interaction as one that represents high risk.			X	

CRYPTOGRAPHIC MODULE					
16	Any cryptographic modules used in client-side authentication **MUST** meet an industry recognized Validation standard (e.g. FIPS 140-3 or comparable).		X	X	
AUTHENTICATION RESULT					
17	The Authentication Service Provider **MUST** return a success result only when the Subject has successfully completed their authentication attempt.	X	X	X	
18	The Authentication Service Provider **MUST** return a failure result to an authentication attempt when the presented Credential is suspended or revoked, or Credential misuse or compromise is detected.	X	X	X	
19	The Authentication Service Provider **MUST** provide a mechanism that: • Confirms that the authentication result was originated by the Authentication Service Provider; • Was not tampered with in transit; and • Is only usable by the Relying Party.		X	X	
20	The authentication result **MUST** be valid for a maximum period of time that is: • Specified by the Authentication Service Provider; and • Known to the Relying Party.		X	X	
INSE	**Authenticated Session Initiation**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
INITIATE SESSION					
1	The Authentication Service Provider **SHOULD** provide the ability to maintain a Session binding with all Relying Parties, where Authenticated Session Initiation is a supported process.	X			
2	The Authentication Service Provider **MUST** provide the ability to maintain a Session binding with all Relying Parties, where Authenticated Session Initiation is a supported process.		X	X	

3	If a Subject authenticates at a given LOA, the resulting Session **MUST** be considered to be the same LOA (e.g., if the Subject authenticates at LOA2, the Session must be considered LOA2), where Authenticated Session Initiation is a supported process.	X	X	X	
RE-AUTHENTICATION					
4	The Authentication Service Provider **SHOULD** require the Subject to re-authenticate after a predefined period of time or event as determined by a risk-based approach (e.g., when a single sign-on attempt is made to another Relying Party in a federation).	X			
5	The Authentication Service Provider **MUST** require the Subject to re-authenticate after a predefined period of time or event as determined by a risk-based approach (e.g., when a single sign-on attempt is made to another Relying Party in a federation or when a Relying Party requests re-authentication).		X	X	
6	The Authentication Service Provider **MAY** extend Session timeouts.	X			
7	If the re-authentication is LOA2 or LOA3, the Session timeouts **MAY** be extended but **MUST** match original LOA and meet all authentication criteria listed above.		X	X	
TESE	**Authenticated Session Termination**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
SESSION TIMEOUT					
1	The Authentication Service Provider **SHOULD** enforce a maximum Session time to force re-authentication in a federated single sign-on scenario after the predefined Session time, where Authenticated Session Termination is a supported process.	X			
2	The Authentication Service Provider **MUST** enforce a maximum Session time to force re-authentication in a federated single sign-on scenario after the predefined Session time, where Authenticated Session Termination is a supported process.		X	X	

3	The Authentication Service Provider **SHOULD** enforce a maximum Session inactivity time to force re-authentication in a federated single sign-on scenario after the predefined Session time, where Authenticated Session Termination is a supported process.	X			
4	The Authentication Service Provider **MUST** enforce a maximum Session inactivity time to force re-authentication in a federated single sign-on scenario after the predefined Session time, where Authenticated Session Termination is a supported process.		X	X	
5	Maximum Session time and maximum Session inactivity values at LOA3 **SHOULD** be shorter than for those for LOA2.			X	
6	A Session timeout due to exceeding maximum Session time or maximum Session inactivity time at LOA3, **MAY** result in either a Session termination, or a downgrade to a LOA2 Session.			X	
7	In the case of a Session downgrade: • The Authentication Service Provider **MUST** notify all Relying Parties associated to the LOA3 Session; and • The Session timeouts due to exceeding maximum Session time or maximum Session inactivity time **MAY** be extended to their LOA2 values (minus the time which has already passed).			X	
TERMINATE SESSION					
8	The Authentication Service Provider **SHOULD** notify all Relying Parties that the Session has been terminated.	X			
9	The Authentication Service Provider **MUST** notify all Relying Parties that the Session has been terminated.		X	X	
CRSP	**Credential Suspension**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
SUBJECT INITIATED					
1	The Credential Service Provider **SHOULD** provide the ability for a Subject to initiate Credential suspension.	X	X	X	
ADMINISTRATOR INITIATED					

2	The Credential Service Provider **MAY** provide the ability for authorized personnel to suspend the use of an Credential.	X	X	X	
3	The Credential Service Provider **SHOULD** enforce access controls to ensure only authorized personnel have access to this process.	X			
4	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.		X	X	
5	The Credential Service Provider **MUST** require authorized personnel to provide a LOA3 or higher Credential in order to suspend the use of an Credential.			X	
CRVY	**Credential Recovery**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
SUBJECT INITIATED					
1	The Credential Service Provider **SHOULD** provide the Subject the ability to request the recovery of a suspended Credential, where Credential Recovery is a supported process.	X			
2	The Credential Service Provider **SHOULD** require the Subject to authenticate with a LOA equivalent to that of the Credential being recovered, where Credential Recovery is a supported process.	X			
3	The Credential Service Provider **MUST** provide the Subject the ability to request the recovery of a suspended Credential, where Credential Recovery is a supported process.		X	X	
4	The Credential Service Provider **MUST** require the Subject to authenticate with a LOA equivalent to that of the Credential being recovered, where Credential Recovery is a supported process.		X	X	
ADMINISTRATOR INITIATED					
5	The Credential Service Provider **MAY** provide the ability for authorized personnel to initiate Credential Recovery on behalf of the Subject.	X	X	X	

6	The Credential Service Provider **SHOULD** enforce access controls to ensure only authorized personnel have access to this process, where Credential Recovery is a supported process.	X			
7	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process, where Credential Recovery is a supported process.		X	X	
8	The Credential Service Provider **MUST** require authorized personnel to provide a LOA3 or higher Credential in order to recover a Credential, where Credential Recovery is a supported process.			X	
SYSTEM INITIATED					
9	The Credential Service Provider **MAY** provide the ability to automatically recover a suspended Credential (e.g., automatically reactivate a Credential previously suspended due to too many failed login attempts).	X	X	X	
CRMA	**Credential Maintenance**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
SUBJECT INITIATED					
1	The Credential Service Provider **SHOULD** provide the ability to update the Authenticators bound to the Credential where possible (e.g., password change, bind a new Authenticator).	X			
2	The Credential Service Provider **SHOULD** provide the ability to allow Credential attributes (e.g., password, Q&A, recovery codes) to be modified.	X			
3	The Credential Service Provider **MUST** provide the ability to update the Authenticators bound to the Credential where possible (e.g., password change, change of PIN, refresh face image on file with more recent image, change of private key).		X	X	
4	The Credential Service Provider **MUST** provide the ability to allow Credential attributes (e.g., password, Q&A, recovery codes, cryptographic keys, biometrics, aliases, DIDs) to be modified.		X	X	

5	The Credential Service Provider **MUST** require authentication at a LOA equivalent to or greater than the LOA of the Credential attribute (e.g., password, Q&A, recovery codes, cryptographic keys, biometrics, aliases, DIDs) being modified. For example, a Subject logged using a single-factor password should not be able to modify recovery codes, OTP values.		X	X	
ADMINISTRATOR INITIATED					
6	The Credential Service Provider **MAY** provide the ability to allow authorized personnel to update the Authenticators bound to the Credential (e.g., remove an Authenticator or initiate a password change).	X	X	X	
7	The Credential Service Provider **MAY** provide the ability to allow authorized personnel to update Credential attributes.	X	X	X	
8	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.	X	X	X	
9	The Credential Service Provider **MUST** require authorized personnel to provide a LOA3 or higher Credential in order to perform Credential maintenance.			X	
10	The Credential Service Provider **SHOULD** require the Subject to complete any administrator initiated Credential activities (e.g., an administrator cannot change the Subjects password only initiate a reset).	X			
11	The Credential Service Provider **MUST** require the Subject to complete any administrator initiated Credential activities (e.g., an administrator cannot change the Subjects password only initiate a reset).		X	X	
SYSTEM INITIATED					
12	The Credential Service Provider **SHOULD** enforce Authenticator control and protection requirements (e.g., Q&A complexity requirements, password updates, OTP updates) appropriate to the Authenticator (see NIST Special Publication 800-53 (Rev. 4) and Government of Canada Password Guidance for examples and references).	X			

13	The Credential Service Provider **MUST** enforce Authenticator control and protection requirements (e.g., Q&A complexity requirements, password updates, OTP updates) appropriate to the Authenticator (see NIST Special Publication 800-53 (Rev. 4) and Government of Canada Password Guidance for examples and references).		X	X	
CRVX	**Credential Revocation**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
SUBJECT INITIATED					
1	The Credential Service Provider **SHOULD** allow a Subject to revoke their own Credential.	X			
2	The Credential Service Provider **MUST** allow a Subject to revoke their own Credential.		X	X	
ADMINISTRATOR INITIATED					
3	The Credential Service Provider **MAY** have the ability to allow authorized personnel to revoke a Credential.	X			
4	The Credential Service Provider **MUST** have the ability to allow authorized personnel to revoke a Credential.		X	X	
5	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.	X	X	X	
6	The Credential Service Provider **MUST** require authorized personnel to provide a LOA3 or higher Credential in order to revoke a Credential.			X	

7. 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
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
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

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
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
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

Table 2. Authentication Use Cases

8. Appendix B: Summary of Trusted Process Conditions

Table 4 summarizes the input and output conditions of the PCTF Authentication 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., 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.
Revoked Credential	The Credential is permanently disabled or deleted. This is a permanent condition.

Table 3. Authentication Component Conditions

9. 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 5 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 Credential	-	Issued Credential
Authentication	Issued Credential	Credential Issuance	Authenticated Credential
Authenticated Session Initiation	Authenticated Credential	Authentication	Authenticated Session
Authenticated Session Termination	Authenticated Session	Authenticated Session Initiation	No Authenticated Session
Credential Suspension	Issued Credential	Credential Issuance	Inaccessible Credential
Credential Recovery	Inaccessible Credential	Credential Suspension	Issued Credential
Credential Maintenance	Issued Credential	Credential Issuance, Authentication	Issued Credential (updated)
Credential Revocation	Inaccessible Credential	Credential Issuance, Authentication	Revoked Credential

Table 4. Trusted Process Relationships

10. 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. <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:

- 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. <https://csrc.nist.gov/publications/detail/fips/140/2/final >
- 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 >
- 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 >
- AXELOS. *ITIL v3 (formerly the Information Technology Infrastructure Library).* 2011. <https://www.axelos.com/best-practice-solutions/itil >

11. Notes

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

12. 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	Approved as Final Recommendation V1.0
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
1.1	2023-12-01	PCTF Authentication Design Team	TFEC approves as Final Recommendation V1.1
1.2	2024-05-10	PCTF Editors & Authentication Design Team	TFEC approves as Final Recommendation v1.2
1.2	2024-07-08	PCTF Editors & Authentication Design Team	Approved as Final Recommendation V1.2 through DIACC Sustaining Member Ballot