PCTF Authentication Conformance Profile Final Recommendation V1.2

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 Conformance Criteria

This document specifies the Conformance Criteria of the PCTF Authentication Component, a component of the Pan-Canadian Trust Framework (PCTF). For a general introduction to the Pan-Canadian 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.

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.

1.1 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.

2. Authentication Conventions

Each PCTF component includes conventions that ensure consistent use and interpretation of terms and concepts appearing in the component. **The PCTF Authentication Component Overview provides conventions for this 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.

2.1 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.

3. 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	• ccidental 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	• 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

					harm Harm to Relying Parties: • Financial harm • Loss of privilege/ access/use • Reputational harm • Privacy harm	
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/utility	• Malicious actors targeting unpatched software • Unusable software (incompatible)	• Holder is unable to perform required transactions • Credential or access compromised	• Product and/or service should be updated or replaced with a compatible and/or more secure replacement and a patch 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	product or service quality risk	Product or service does not implement, or	• Product or service is unable to	• Product or service	• Denial of Service	• Product or service implements industry standards as

management → user inconvenience.		conform to, industry standards	interoperate with applications or other systems	provider	to the Customer • Holder is unable to perform required transactions • Issuer unable to issue • Verifier not able to verify	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	• 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

					to issue unauthorized Credentials or to bypass access controls	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 security → harm to Subjects	Backup and recovery risks/key management risks	Product or service has inadequate backup and recovery controls	• Malicious actor steals secret keys using backup/recovery mechanism	• Malicious actor (local or remote)	• Compromised keys/unauthorized data access/privacy breach/identity theft	• Backup and recovery processes to be defined for 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 managem	Infrastructure, software or device-related security	Product or service does not support required security	• Product or services software does not have	• Malicious actor (local or	• Compromised keys/una	• Product or service uses adequate/evaluated key management

ent security → harm to Subjects	risks/key management risks	functions for specific/target LOA(s).	adequate key management protections. • Malicious actor steals secret keys (e.g., steals key from memory, cracks white box crypto, power analysis)	remote)	uthorized data access/privacy breach/identity theft	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 → harm to Subject	Unauthorized use of the product or service	Authenticator compromise	• When users share devices, authenticators without proper access controls could allow others to share the information of the authorized holder without their consent	• Hackers • Acquaintances • Family Members	• Assertions are made on the behalf of the user without their consent	• Include specific language in the EULA to ensure authorized users understand 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	• Holder provides more information to Verifier than they would	• Product or service effectively discloses information to be shared to Holder and allows Holder to control • Data that may not be 'understandable' (i.e.,

				user of specific Products or Services that do not offer proper notice	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	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	• Product or service implements industry standard accessibility capabilities

					disabilities; Subject vulnerable population to alternate processes or tools that may carry 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	Governance	Product or service relies on (trusts) a	• Product or Service trusts public key of	• Malicious actor that establishes a	• Users make unintentio	• Product or service authenticates Data

registry security → harm to Subject		credential authority that is not (or no longer) appropriate	malicious actor	rogue data registry or registry entry	nal/uninformed sharing decisions • Privacy breach/identity theft	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 session hijacking	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
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

4. 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** ~~:~~ 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	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	

Table 1. PCTF Authentication Component Conformance Criteria

---

5. Revision History

Version	Date of Issue	Author(s)	Description
.01	2018-04-10	TFEC	Initial working draft
.02	2018-07-31	DIACC Editor	Suggested changes to address outstanding review comments.
.03	2019-04-30	DIACC Editor	• Formatting edits • Updated links to referenced standards
.04	2019-07-08	DIACC Editor	• Standardize priority of requirement terms • Update PCTF model image
.05	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

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 Editor and Authentication Design Team	TFEC approves as a Candidate for 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