PCTF Authentication Conformance Profile

Document Status: Final Recommendation V1.0

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

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

Table of Contents

1 Introduction to the PCTF Authentication Component 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

Note

- 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.

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

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: “BASE1” refers to “Baseline Conformance Criteria reference No. 1”.

Note

- 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.

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	Level 2	Level 3	Level 4
BASE	**Baseline**				
EVENT LOGGING					
1	Authentication Credential management and use events **MAY** be logged and retained. If retained, Authentication Credential management and use event logs **MUST** be retained for a predefined period as evidence.	Y			
2	Authentication Credential management and use events **MUST** be logged and retained for a predefined period of time as evidence.		Y	Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	**Level 2**	**Level 3**	**Level 4**
3	Authentication Credential management and use event logs **MUST** be: 1. Traceable back to a specific Authentication Credential and include the result and date and time of the logged event. 2. 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).		Y	Y	
4	Authentication Credential management and use event logs **MUST** have a tamper-detection mechanism to detect unauthorized modifications.		Y	Y	
5	Personal information and authenticator secrets (e.g., passwords, OTP values, security questions, security answers) **MUST NOT** be logged within the service.	Y	Y	Y	
INFORMATION SECURITY					
6	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.	Y			

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	**Level 2**	**Level 3**	**Level 4**
7	The Credential Service Provider/Authentication Service Provider **MUST**: 1. 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. 2. Have an auditable process to demonstrate adherence to a set of information security guidelines and controls.		Y	Y	
8	The Credential Service Provider/Authentication Service Provider **MUST** have an independently audited process to demonstrate adherence to a set of information security guidelines and controls.			Y	
IT SERVICE MANAGEMENT					
9	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.	Y			

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	Level 2	Level 3	Level 4
10	The Credential Service Provider/Authentication Service Provider **MUST**: 1. Establish and maintain a documented service management practice for all aspects of the service it provides related to PCTF Authentication Component Trusted Processes. 2. Have an auditable process to demonstrate adherence a service management practice for all aspects of the service it provides related to PCTF Authentication Component Trusted Processes.		Y		
11	The Credential Service Provider/Authentication Service Provider **MUST**: 1. Establish and maintain a documented service management practice for all aspects of the service it provides related to PCTF Authentication Component Trusted Processes. 2. Have a documented and independently audited service management practice for all aspects of the service it provides related to PCTF Authentication Component Trusted Processes.			Y	
12	The Credential Service Provider/Authentication Service Provider **SHOULD** adhere to an industry standard service management framework (e.g., ITIL).	Y	Y		
13	The Credential Service Provider/Authentication Service Provider **MUST** adhere to an industry standard service management framework (e.g., ITIL).			Y	
MONITORING					

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	**Level 2**	**Level 3**	**Level 4**
14	The Credential Service Provider/Authentication Service Provider **SHOULD** have the ability to monitor the service for indications or evidence of potential Authentication Credential misuse or compromise.	Y			
15	The Credential Service Provider/Authentication Service Provider **MUST** have the ability to monitor the service for indications or evidence of potential Authentication Credential misuse or compromise.		Y	Y	
16	The Credential Service Provider/Authentication Service Provider **SHOULD** take measures to detect misuse of the Authentication Credential.	Y			
17	The Credential Service Provider/Authentication Service Provider **MUST** take measures to detect misuse of the Authentication Credential.		Y	Y	
18	The Credential Service Provider **SHOULD** initiate the Authentication Credential Suspension process, the Authentication Credential Maintenance process, or the Authentication Credential Revocation process when it finds actionable indications of Credential misuse or compromise.	Y			
19	The Credential Service Provider **MUST** initiate the Authentication Credential Suspension process, the Authentication Credential Maintenance process, or the Authentication Credential Revocation process when it finds actionable indications of Authentication Credential misuse or compromise.		Y	Y	
PRIVACY					

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	Level 2	Level 3	Level 4
20	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.	Y			
21	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.		Y	Y	
22	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.		Y	Y	
NOTIFICATIONS					
23	The Credential Service Provider **MAY** notify the Subject of any changes to Authentication Credential information (e.g., password update, adding or removing Authenticators).	Y			
24	The Credential Service Provider **MUST** notify the Subject without undue delay of any changes to Authentication Credential information (e.g., password update, adding or removing authenticators).		Y	Y	
CDIS	**Credential Issuance**				
BINDING SUBJECT					
1	The Credential Service Provider **SHOULD** enforce that the Authentication Credential is only bound to one Subject.	Y			
2	The Credential Service Provider **MUST** enforce that the Authentication Credential is only bound to one Subject.		Y	Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	**Level 2**	**Level 3**	**Level 4**
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 Authentication Credential was issued.	Y			
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 Authentication Credential was issued.		Y	Y	
5	The Credential Service Provider **MUST** make information available to Authentication Service Providers about the current state of all Authentication Credentials it has issued (e.g., if a credential is an "Inaccessible Credential" or a "Revoked Credential", this status information **MUST** be available to Authentication Service Providers).	Y	Y	Y	
BINDING AUTHENTICATORS					
6	The Credential Service Provider **MAY** provide the ability to bind a Subject-provided Authenticator to the Authentication Credential.	Y	Y	Y	
7	The Credential Service Provider **MUST** bind at least one Authenticator to the Authentication Credential. (e.g., password, Q&A, or OTP).	Y	Y	Y	
8	At least two different Authenticators **SHOULD** be bound to the Authentication Credential such that recovery of one authenticator (e.g., from loss or theft) is possible using another Authenticator.		Y		
9	At least two different Authenticators **MUST** be bound to the Authentication Credential such that recovery of the primary Authenticator (e.g., from loss or theft) is possible using another Authenticator.			Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	**Level 2**	**Level 3**	**Level 4**
10	Additional Authenticators, which could be used for recovery purposes, **MUST** be the same or higher LOA as an Authenticator to be recovered.		Y	Y	
11	The Credential Service Provider **MAY** document, or have a documented process for, demonstrating the Level of Assurance of the Subject's identity when the Authentication Credential was recovered.	Y			
12	The Credential Service Provider **MUST** document, or have a documented process for, demonstrating the Level of Assurance of the Subject's identity when the Authentication Credential was recovered.		Y	Y	
AUTHENTICATOR CREATION					
13	When the Authenticator is created (e.g., hardware OTP device OR software OTP), the creator **MUST** have an auditable quality management system or processes.		Y		
14	When the Authenticator is created (e.g., hardware OTP device OR software OTP), the creator **MUST** have an Independently Audited quality management system or processes.			Y	
15	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 process that protects that information from compromise beginning from manufacture time through delivery to the Credential Service Provider.		Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	Level 2	Level 3	Level 4
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 Independently Audited security management process that protects that information from compromise beginning from manufacture time through delivery to the Credential Service Provider.			Y	
AUTHENTICATION CREDENTIAL STORAGE					
17	The Credential Service Provider/Authentication Service Provider **MUST** enforce access controls to prevent unauthorized access to Authentication Credential information.	Y	Y	Y	
18	Any secrets bound to the Authentication Credential **MUST** be either stored as a salted hash or stored encrypted.		Y	Y	
19	Any Authentication Credential attributes containing personal information that are stored within the service **MUST** be secured (e.g., encrypted and/or hashed).	Y	Y	Y	
20	Backups of Authentication Credential information **MUST** be encrypted prior to being transferred to long term storage and **MUST** remain encrypted while in storage.		Y	Y	
21	Cryptographic modules **MUST** meet an industry recognized Validation standard (e.g., FIPS 140-2).		Y	Y	
AUTH	**Authentication**				
AUTHENTICATORS					
1	The Authentication Service Provider **MUST** require at least a single Authenticator be bound to an Authentication Credential.	Y	Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	**Level 2**	**Level 3**	**Level 4**
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.		Y		
3	The Authentication Service Provider **MUST** require at least two different Authenticators that: 1. Provide different Authentication Factors. 2. Are not susceptible to the same threat vectors.			Y	
4	Of the different Authenticators required by the Authentication Service Provider per AUTH3: 1. One of the Authenticators **MUST** be of the type "something the Subject has". 2. The other Authenticator(s) **MAY** be an Authenticator Type that is either "something the Subject knows" or "something the Subject is or does".			Y	
5	The Authentication Service Provider **MUST** consult any information made available by the Credential Service Provider to determine the current state of an Authentication Credential.	Y	Y	Y	
AUTHENTICATOR TYPE					
6	Any Authenticator Type is acceptable.	Y			
7	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).		Y	Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	**Level 2**	**Level 3**	**Level 4**
8	The Authentication Service Provider **MUST** use Authenticator Types that are resistant to the threats listed in **AUTH13**.			Y	
THREAT MITIGATION					
9	The Authentication Service Provider **MUST** be capable of defending against 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 **BASE6**.	Y			
10	The Authentication Service Provider **MUST** be capable of defending against at least the following types of attacks: Authenticator secret guessing, replay, eavesdropping, and Session hijacking. This **MUST** be included in the scope of the auditable process described in **BASE7.**		Y		
11	The Authentication Service Provider **MUST** be capable of defending against 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 **BASE8**.			Y	
ADAPTIVE RISK					
12	The Authentication Service Provider **MAY** provide the ability to perform Adaptive Risk Authentication.	Y			
13	The Authentication Service Provider **SHOULD** provide the ability to perform Adaptive Risk Authentication.		Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	**Level 2**	**Level 3**	**Level 4**
14	The Authentication Service Provider **MUST** detect and mitigate interactions that represent higher-than-typical 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 the greatest possible risk that the Authentication Service Provider can support for such an interaction.			Y	
CRYPTOGRAPHIC MODULE					
15	Any cryptographic modules used in client-side authentication **MUST** meet an industry recognized Validation standard (e.g., FIPS 140-2 or equivalent).		Y	Y	
AUTHENTICATION RESULT					
16	The Authentication Service Provider **MUST** return a success result only when the Subject has successfully completed their authentication attempt.	Y	Y	Y	
17	The Authentication Service Provider **MUST** return a failure result to an authentication attempt when the presented Authentication Credential is suspended or revoked, or Authentication Credential misuse or compromise is detected.	Y	Y	Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	Level 2	Level 3	Level 4
18	The Authentication Service Provider **MUST** provide a mechanism that: 1. Confirms that the authentication result was originated by the Authentication Service Provider 2. Was not tampered with in transit 3. Is only usable by the Relying Party		Y	Y	
19	The authentication result **MUST** be valid for a maximum period of time that is i) specified by the Authentication Service Provider and ii) known to the Relying Party.		Y	Y	
INSE	**Authenticated Session Initiation**				
INITIATE SESSION					
1	The Authentication Service Provider **SHOULD** provide the ability to maintain a Session binding with all Relying Parties.	Y			
2	The Authentication Service Provider **MUST** provide the ability to maintain a Session binding with all Relying Parties.		Y	Y	
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).	Y	Y	Y	
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).	Y			

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	Level 2	Level 3	Level 4
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).		Y	Y	
6	The Authentication Service Provider **MAY** extend Session timeouts.	Y			
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.		Y	Y	
TESE	**Authenticated Session Termination**				
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.	Y			
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.		Y	Y	
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.	Y			
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.		Y	Y	
5	Maximum Session time and maximum Session inactivity values at LOA3 **SHOULD** be shorter than for those for LOA2.			Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	Level 2	Level 3	Level 4
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.			Y	
7	In the case of a Session downgrade: 1. the Authentication Service Provider **MUST** notify all Relying Parties associated to the LOA3 Session; and 2. 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).			Y	
TERMINATE SESSION					
8	The Authentication Service Provider **SHOULD** notify all Relying Parties that the Session has been terminated.	Y			
9	The Authentication Service Provider **MUST** notify all Relying Parties that the Session has been terminated.		Y	Y	
CRSP	**Authentication Credential Suspension**				
SUBJECT INITIATED					
1	The Credential Service Provider **SHOULD** provide the ability for a Subject to suspend the use of its Authentication Credential.	Y	Y	Y	
ADMINISTRATOR INITIATED					
2	The Credential Service Provider **MAY** provide the ability for authorized personnel to suspend the use of an Authentication Credential.	Y	Y	Y	
3	The Credential Service Provider **SHOULD** enforce access controls to ensure only authorized personnel have access to this process.	Y			

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	Level 2	Level 3	Level 4
4	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.		Y	Y	
5	The Credential Service Provider **MUST** require authorized personnel to provide a LOA3 or higher Authentication Credential in order to suspend the use of an Authentication Credential.			Y	
CRVY	**Authentication Credential Recovery**				
SUBJECT INITIATED					
1	The Credential Service Provider **SHOULD** provide the ability to recover a lost or suspended Authentication Credential.	Y			
2	The Credential Service Provider **SHOULD** require the Subject to authenticate with a LOA equivalent to that of the Authentication Credential being recovered.	Y			
3	The Credential Service Provider **MUST** provide the ability to recover a lost or suspended Authentication Credential.		Y	Y	
4	The Credential Service Provider **MUST** require the Subject to authenticate with a LOA equivalent to that of the Authentication Credential being recovered.		Y	Y	
ADMINISTRATOR INITIATED					
5	The Credential Service Provider **MAY** provide the ability for authorized personnel to initiate Authentication Credential Recovery on behalf of the Subject.	Y	Y	Y	
6	The Credential Service Provider **SHOULD** enforce access controls to ensure only authorized personnel have access to this process.	Y			

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

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	**Level 2**	**Level 3**	**Level 4**
5	The Credential Service Provider **MUST** require authentication at a LOA equivalent to or greater than the LOA of the Authentication 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.		Y	Y	
ADMINISTRATOR INITIATED					
6	The Credential Service Provider **MAY** provide the ability to allow authorized personnel to update the Authenticators bound to the Authentication Credential (e.g., remove an Authenticator or initiate a password change).	Y	Y	Y	
7	The Credential Service Provider **MAY** provide the ability to allow authorized personnel to update Authentication Credential attributes.	Y	Y	Y	
8	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.	Y	Y	Y	
9	The Credential Service Provider **MUST** require authorized personnel to provide a LOA3 or higher Authentication Credential in order to perform Authentication Credential maintenance.			Y	
10	The Credential Service Provider **SHOULD** require the Subject to complete any administrator initiated Authentication Credential activities (e.g., an administrator cannot change the Subjects password only initiate a reset).	Y			

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	Level 2	Level 3	Level 4
11	The Credential Service Provider **MUST** require the Subject to complete any administrator initiated Authentication Credential activities (e.g., an administrator cannot change the Subjects password only initiate a reset).		Y	Y	
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).	Y			
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).		Y	Y	
CRVX	**Authentication Credential Revocation**				
SUBJECT INITIATED					
1	The Credential Service Provider **SHOULD** allow a Subject to revoke their own Authentication Credential.	Y			
2	The Credential Service Provider **MUST** allow a Subject to revoke their own Authentication Credential.		Y	Y	
ADMINISTRATOR INITIATED					
3	The Credential Service Provider **MAY** have the ability to allow authorized personnel to revoke an Authentication Credential.	Y			
4	The Credential Service Provider **MUST** have the ability to allow authorized personnel to revoke an Authentication Credential.		Y	Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
		Level 1	**Level 2**	**Level 3**	**Level 4**
5	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.	Y	Y	Y	
6	The Credential Service Provider **MUST** require authorized personnel to provide a LOA3 or higher Authentication Credential in order to revoke an Authentication Credential			Y	

Table 1. PCTF Authentication Component Conformance Criteria

4 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