PCTF Verified Login Conformance Profile Draft Recommendation V1.0

This Draft Recommendation has been developed by the Digital ID & Authentication Council of Canada (DIACC) Trust Framework Expert Committee (TFEC). The TFEC operates under the controlling policies of the DIACC. Comments submitted by the public are subject to the DIACC Contributor Agreement.

DIACC expects to modify and improve this Draft Recommendation based upon public comments. The purpose of the open commentary is to ensure transparency in development and diversity of truly Pan-Canadian input. Comments made during the review will be considered for incorporation to the next draft. DIACC will prepare a disposition of comments to provide transparency with regard to how each comment was handled.

Forthcoming PCTF releases will expand, clarify, and refine the content of this document.

Contents

1 Introduction to the PCTF Verified Login Conformance Criteria

This document specifies the Conformance Criteria of the PCTF Verified Login 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 are used to ensure that Verified Login Trusted Processes result in the representation of a unique subject and a Level of Assurance that it is the same subject with each successful login to an Authentication Service Provider. Relying parties can then rely upon the assurance to uniquely identify the subject within their application or program space.

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 audited 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 are intended to complement existing legislation and regulations. Digital identity ecosystem participants are expected meet the legislative and regulatory requirements (e.g., all privacy laws and regulations) applicable in their jurisdictions. For example, any entity carrying out a Verified Login Trusted Process that has access to a Subject's personal information is bound by applicable privacy laws.

2 Verified Login Conventions

Each PCTF component includes conventions that ensure consistent use and interpretation of terms and concepts appearing in the component. **The PCTF Verified Login 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 Verified Login Component Overview and the PCTF Glossary apply. Key terms and concepts described and defined in this section, or the PCTF Verified Login 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 not choosing to adhere to the conformance criteria or choosing a different option as specified by the conformance criteria.
- **SHOULD NOT** means that valid reasons 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 Verified Login Conformance Criteria

The following sections define Conformance Criteria that are essential requirements for the Trusted Processes of Verified Login Component. The Verified Login 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: “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 Verified Login 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 Verified Login 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)			
BASE	**Baseline**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
EVENT LOGGING					
1	Credential management and use events **MAY** be logged and **MAY** be retained for a predefined period of time as evidence.	Y			
2	Credential management and use events **MUST** be logged and retained for a predefined period of time as evidence. The log **MUST** be traceable back to a specific Credential and include the result and date and time of the event. The logs **MUST** be protected by access controls to limit access only to those who require it.		Y	Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
3	The logs **MUST** have a tamper-detection mechanism to detect unauthorized modifications.			Y	
4	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					
5	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			
6	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. The Credential Service Provider/Authentication Service Provider **MUST** have an auditable process to demonstrate adherence to a set of information security guidelines and controls.		Y		
7	In addition to the LOA2 requirements, the Credential Service Provider/Authentication Service Provider **MUST** have an independently audited process to demonstrate adherence.			Y	
IT SERVICE MANAGEMENT					
8	The Credential Service Provider/Authentication Service Provider **SHOULD** have a documented service management practice for all aspects of the service it provides related to verified login Trusted Processes.	Y			
9	The Credential Service Provider/Authentication Service Provider **MUST** have a documented and auditable service management practice for all aspects of the service it provides related to verified login Trusted Processes.		Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
10	The Credential Service Provider/Authentication Service Provider **MUST** have a documented and independently audited service management practice for all aspects of the service it provides related to verified login Trusted Processes.			Y	
11	The Credential Service Provider/Authentication Service Provider **SHOULD** adhere to an industry standard service management framework, such as ITIL.	Y	Y		
12	The Credential Service Provider/Authentication Service Provider **MUST** adhere to an industry standard service management framework such as ITIL.			Y	
MONITORING					
13	The Credential Service Provider/Authentication Service Provider **SHOULD** have the ability to monitor the service for indications or evidence of potential Credential misuse or compromise.	Y			
14	The Credential Service Provider/Authentication Service Provider **MUST** have the ability to monitor the service for indications or evidence of potential Credential misuse or compromise.		Y	Y	
15	The Credential Service Provider/Authentication Service Provider **SHOULD** take measures to detect actual misuse of the Credential.	Y			
16	The Credential Service Provider/Authentication Service Provider **MUST** take measures to detect actual misuse of the Credential.		Y	Y	
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.	Y			
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.		Y	Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
PRIVACY					
19	The Credential Service Provider/Authentication Service Provider **SHOULD** adhere to the privacy risk management practices of the PCTF and any selected Conformance Profiles.	Y			
20	The Credential Service Provider/Authentication Service Provider **MUST** adhere to the privacy risk management practices of the PCTF and any selected Conformance Profiles.		Y	Y	
21	The Credential Service Provider/Authentication Service Provider **MUST** adhere to the privacy risk management practices that are accepted by all parties participating in the digital ID service.		Y	Y	
NOTIFICATIONS					
22	The Credential Service Provider **MAY** notify the Subject of any changes to Credential information (e.g., password update, adding or removing Authenticators).	Y			
23	The Credential Service Provider **SHOULD** notify the Subject of any changes to Credential information (e.g., password update, adding or removing authenticators).		Y		
24	The Credential Service Provider **MUST** notify the Subject of any changes to Credential information (e.g., password update, adding or removing authenticators).			Y	
CDIS	**Credential Issuance**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
BINDING A SUBJECT					
1	The Credential Service Provider **SHOULD** enforce that the Credential is only bound to one Subject.	Y			
2	The Credential Service Provider **MUST** enforce that the Credential is only bound to one Subject.		Y	Y	
3	The Credential Service Provider **MAY** document the Level of Assurance of the Subject's identity when the Credential was issued.	Y	Y	Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
4	The Credential Service Provider **MUST** make information available to Authentication Service Providers about the current state of all 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					
5	The Credential Service Provider **MAY** provide the ability to bind a Subject-provided Authenticator to the Credential.	Y	Y	Y	
6	The Credential Service Provider **MUST** bind at least one Authenticator to the Credential. (e.g., password, Q&A, or OTP).	Y	Y	Y	
7	At least two different Authenticators **SHOULD** be bound to the Credential such that recovery of one from loss or theft is possible using another Authenticator.		Y		
8	At least one additional Authenticator **MUST** exist and be bound to the Credential such that recovery of the primary Authenticator (e.g., from loss or theft of the primary Authenticator) is possible.			Y	
9	Additional Authenticators, which could be used for recovery purposes, **MUST** be the same or higher LOA as the Authenticator to be recovered.		Y	Y	
AUTHENTICATOR CREATION					
10	When the Authenticator is created (e.g., hardware OTP device OR software OTP), the creator **MUST** have an auditable quality management process.		Y		
11	When the Authenticator is created (e.g., hardware OTP device OR software OTP), the creator **MUST** have an Independently Audited quality management process.			Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
12	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		
13	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	
CREDENTIAL STORAGE					
14	The Credential Service Provider/Authentication Service Provider **SHOULD** enforce access controls to prevent unauthorized access to the Credential information.	Y			
15	The Credential Service Provider/Authentication Service Provider **MUST** enforce access controls to prevent unauthorized access to the Credential information.		Y	Y	
16	Any secrets bound to the Credential **MUST** be either stored as a salted hash or stored encrypted.		Y	Y	
17	Any Credential attributes containing personal information that are stored within the service **MUST** be secured (e.g., encrypted and/or hashed).	Y	Y	Y	
18	Backups of Credential information **MUST** be encrypted prior to being transferred to long term storage and **MUST** remain encrypted while in storage.		Y	Y	
19	Cryptographic modules **MUST** meet an industry recognized validation standard (e.g., FIPS 140-2).			Y	

Reference	Conformance Criteria	Level of Assurance (LOA)			
AUTH	**Authentication**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
AUTHENTICATORS					
1	The Authentication Service Provider **MUST** require at least a single Authenticator be bound to a Credential.	Y	Y		
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". "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 i) provide different Authentication Factors and ii) are not susceptible to the same threat vectors.			Y	
4	One of the Authenticators **MUST** be of type that is "something the Subject has". 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 a Credential.	Y	Y	Y	
6	The Authentication Service Provider **SHOULD NOT** indicate a successful authentication result (Authenticated Credential) where the presented Credential is an Inaccessible Credential or a Revoked Credential.	Y			
7	The Authentication Service Provider **MUST NOT** indicate a successful authentication result (Authenticated Credential) where the presented Credential is an Inaccessible Credential or a Revoked Credential		Y	Y	
AUTHENTICATOR TYPE					
8	Any Authenticator Type is acceptable.	Y			

Reference	Conformance Criteria	Level of Assurance (LOA)			
9	The Authentication Service Provider **MUST** utilize industry standard or industry best practice for authentication (e.g., standards developed and approved by Kantara, W3C, IETF or FIDO Alliance).		Y	Y	
10	The Authentication Service Provider **MUST** use Authenticator Types that are resistant to the threats listed in **AUTH13**.			Y	
THREAT MITIGATION					
11	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 **BASE5**.	Y			
12	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 **BASE6.**		Y		
13	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 independently audit process required by **BASE7**.			Y	
ADAPTIVE RISK					
14	The Authentication Service Provider **MAY** provide the ability to perform Adaptive Risk Authentication.	Y			
15	The Authentication Service Provider **SHOULD** provide the ability to perform Adaptive Risk Authentication.		Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
16	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					
17	Any cryptographic modules used in client-side authentication **MUST** meet an industry recognized validation standard (e.g., FIPS 140-2 or equivalent).			Y	
AUTHENTICATION RESULT					
18	The Authentication Service Provider **MUST** return a success only when the Subject has successfully completed their authentication attempt.	Y	Y	Y	
19	The Authentication Service Provider **MUST** return failure to an authentication attempt when the presented Credential is suspended or revoked or Credential misuse or compromise is detected.	Y	Y	Y	
20	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	
21	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	

Reference	Conformance Criteria	Level of Assurance (LOA)			
INSE	**Authenticated Session Initiation**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
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 the Subject authenticates at LOA2, the session **MUST** be considered LOA2.		Y		
4	If the Subject authenticates at LOA3, the session **MUST** be considered LOA3.			Y	
RE-AUTHENTICATION					
5	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			
6	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	
7	The Authentication Service Provider **MAY** extend session timeouts.	Y			
8	If the re-authentication is at least LOA2, the session timeouts **MAY** be extended but **MUST** match original level and meet all authentication criteria listed above.		Y		
9	If the re-authentication is at least LOA3, the session timeouts **MAY** be extended but **MUST** match original level and meet all authentication criteria listed above.			Y	
TESE	**Authenticated Session Termination**	**Level 1**	**Level 2**	**Level 3**	**Level 4**

Reference	Conformance Criteria	Level of Assurance (LOA)			
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	
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	

Reference	Conformance Criteria	Level of Assurance (LOA)			
CRSP	**Credential Suspension**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
SUBJECT INITIATED					
1	The Credential Service Provider **SHOULD** provide the ability for a Subject to suspend the use of its Credential.	Y	Y	Y	
HUMAN INITIATED					
2	The Credential Service Provider **MAY** provide the ability for authorized personnel to suspend the use of a Credential.	Y	Y	Y	
3	The Credential Service Provider **SHOULD** enforce access controls to ensure only authorized personnel have access to this process.	Y			
4	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.		Y	Y	
5	In addition to requirements specified for LOA2, the Credential Service Provider **MUST** require authorized personnel to provide a LOA3 or higher Credential in order to suspend the use of a Credential.			Y	
CRVY	**Credential Recovery**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
SUBJECT INITIATED					
1	The Credential Service Provider **SHOULD** provide the ability to recover a lost or suspended Credential.	Y			
2	The Credential Service Provider **SHOULD** require the Subject to authenticate with a LOA equivalent to that of the Credential being recovered.	Y			
3	The Credential Service Provider **MUST** provide the ability to recover a lost or suspended Credential.		Y	Y	
4	The Credential Service Provider **MUST** require the Subject to authenticate with a LOA equivalent to that of the Credential being recovered.		Y	Y	
HUMAN INITIATED					

Reference	Conformance Criteria	Level of Assurance (LOA)			
5	The Credential Service Provider **MAY** provide the ability for authorized personnel to initiate a 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			
7	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.		Y	Y	
8	In addition to requirements specified for LOA2, the Credential Service Provider **MUST** require authorized personnel to provide a LOA3 or higher Credential in order to recover a Credential.			Y	
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).	Y	Y	Y	
CRMA	**Credential Maintenance**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
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).	Y			
2	The Credential Service Provider **SHOULD** provide the ability to allow the 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 Credential where possible (e.g., password change, change of PIN, refresh face image on file with more recent image, or change of private key)		Y	Y	
4	The Credential Service Provider **MUST** provide the ability to allow the 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)**			
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.		Y	Y	
HUMAN 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).	Y	Y	Y	
7	The Credential Service Provider **MAY** provide the ability to allow authorized personnel to update the 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	In addition to requirements specified for LOA2, the Credential Service Provider **MUST** require authorized personnel to provide a LOA3 or higher Credential in order to perform Credential maintenance.			Y	
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).	Y			
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).		Y	Y	
SYSTEM INITIATED					
12	The Credential Service Provider **SHOULD** enforce Authenticator complexity requirements and periodic Authenticator refresh (e.g., Q&A complexity requirements, password updates, OTP updates).	Y			

Reference	Conformance Criteria	Level of Assurance (LOA)			
13	The Credential Service Provider **MUST** enforce Authenticator complexity requirements and periodic Authenticator refresh (e.g., Q&A complexity requirements, password updates, OTP updates).		Y	Y	
CRVX	**Credential Revocation**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
SUBJECT INITIATED					
1	The Credential Service Provider **SHOULD** allow a Subject to revoke their own Credential.	Y			
2	The Credential Service Provider **MUST** allow a Subject to revoke their own Credential.		Y	Y	
HUMAN INITIATED					
3	The Credential Service Provider **MAY** have the ability to allow authorized personnel to revoke a Credential.	Y			
4	The Credential Service Provider **MUST** have the ability to allow authorized personnel to revoke a Credential.		Y	Y	
5	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.	Y	Y	Y	
6	In addition to requirements specified for LOA2, the Credential Service Provider **MUST** require authorized personnel to provide a LOA3 or higher Credential in order to revoke a Credential			Y	

Table 1. PCTF Verified Login Component Conformance Criteria