Verified Login Conformance Profile Discussion Draft Version 0.03

This Discussion Draft 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 Discussion Draft based upon public comments. The purpose of the open commentary is to ensure transparency in development and diversity of a 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. The intended target audience is inclusive of decision makers who may or may not be domain technology experts.

When reviewing this draft, please consider the following:

1. Do the standards referenced in the document (i.e. Canadian Security Establishment ITSP.30.031 V3, US NIST 800-63-3, and UK GPG-44) continue to be the ones referenced in the Verified Login. Are there alternative or more recent standards and guidelines that should be referenced along with or instead of the ones listed?
2. Do you agree with the current name of the component – Verified Login; or is there an alternate name such as Verified Credential that would be more appropriate?
3. Do you agree with the list of Trusted Processes for Verified Login?
4. Is the description of the Trusted Processes clear and accurate?
5. Are the conformance criteria clear and measurable/assessable?
6. Do you agree with the terms used to describe Verified Login as they are presented in the document?

Table of Contents

1 Introduction to Verified Login Conformance Criteria

This document specifies the set of agreed upon conformance criteria for the Verified Login Component, a component of the Pan-Canadian Trust Framework. The Verified Login Conformance Profile is the agreed upon criteria that are used to ensure that 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 the credential service provider. Relying parties can then rely upon the assurance to uniquely identify the subject within their application or program space.

Conformance criteria are central to a trust framework because they specify the essential requirements agreed to by the trust framework participants to ensure the integrity of their processes. This integrity is paramount because the output or result of a Trusted Process is relied on by many participants – over time and across organizational, jurisdictional and sectoral boundaries.

1.1 Relationship to the Pan-Canadian Trust Framework

The Pan-Canadian Trust Framework (PCTF) consists of a set of modular or functional components that can be independently assessed and certified for consideration as trusted components. Building on a Pan-Canadian approach, the PCTF enables the public and private sector to work collaboratively to safeguard digital identities by standardizing processes and practices across the Canadian digital ecosystem.

Figure 1 is an illustration of the Pan-Canadian Trust Framework Model Visual Draft. The processes of the Verified Login Component are performed by participants in the Create & Manage Digital Identities as well as the Use Digital Identity categories.

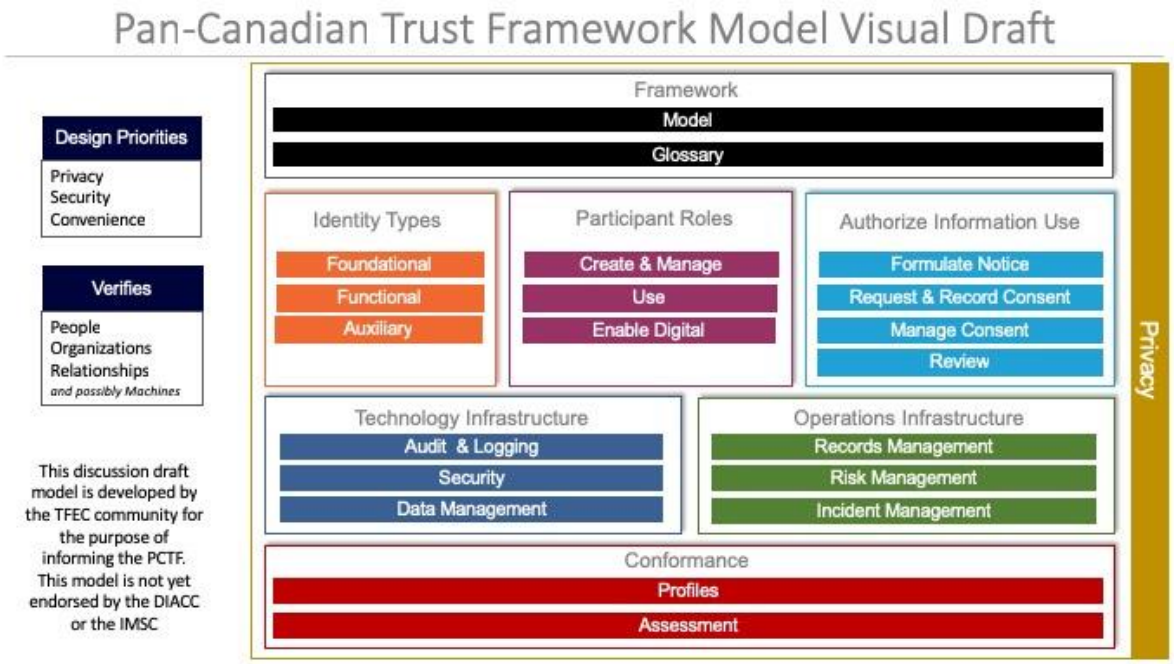

Figure 1. Pan-Canadian Trust Framework Model Visual Draft

1.2 Keywords and Definitions

To ensure consistent application, keywords that appear in **bold** in the conformance criteria are to be interpreted as follows:

- **MUST**, **REQUIRED**, or **SHALL** means that the requirement is absolute as part of the conformance criteria.
- **MUST NOT** or **SHALL NOT** means that the requirement is an absolute prohibition of the conformance criteria.
- **SHOULD** or **RECOMMENDED** 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** or **NOT RECOMMENDED** means that valid 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** or **OPTIONAL** means that the requirement is discretionary but recommended.

Additional keywords, such as normative definitions in related standards and specification, will also be indicated in **bold**.

1.3 Related Standards and Supporting Documentation

The intent of the PCTF, and specifically Verified Login, is to develop Canadian standards that will allow citizens and consumers to interact with private sector and public sector organizations with trust and confidence. There is similar work in progress, or completed, elsewhere in the world and within the Canadian public sector dealing with authentication standards. Instead of re-inventing new standards, Verified Login should look to leverage the experience and lessons learned by other governments and organizations that have been actively developing and evolving these processes and standards. Verified Login has taken guidance from and is based upon the following standards and guidance documents:

- ITSP.30.031 v3 User Authentication Guidance For Information Technology System (ITSP.30.031)
- NIST 800-63-3 Digital Identity Guidelines (800-63-3, 800-63A, 800-63B, and 800-63C)
- Good Practice Guide No. 44 Authentication and Credentials for use with HMG Online Service (GPG-44)

The reader is encouraged to read the above documents to get a deeper understanding of authentication processes, standards and conformance criteria that have been developed in other jurisdictions.

A note about biometrics: Given the inherent lack of revocability of biometrics, biometrics are generally viewed in the above standards as a means to unlock an authenticator within a local device to facilitate remote authentication with a service. One example includes using Apple TouchID to unlock access to a mobile one-time passcode or some other locally stored and generated mobile authenticator.

NIST 800-63 describes the use of biometrics as follows: "A biometric also does not constitute a secret. Accordingly, these guidelines only allow the use of biometrics for authentication when strongly bound to a physical authenticator."

ITSP.30.031 describes the use of biometrics as follows: "Something a user is or does may be replicated. A threat actor may obtain a copy of the token owner's fingerprint and construct a replica - assuming that the biometric system(s) employed do not block such attacks by employing robust liveness detection techniques." and "Automated recognition of individuals based on their behavioural and biological characteristics. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration."

Based upon the above guidance from NIST and ITSP, Verified Login will at this time consider biometric authentication only in the context of unlocking access to another authenticator, with the most popular example being unlocking access through biometric to a mobile authenticator.

1.4 Definitions

For the purposes of the Verified Login Component documents, the following definitions are used:

- **Adaptive Risk –** Dynamic measure of the risk associated with a transaction or service access based on context and behaviour.
- **Adaptive Risk Authentication –** Dynamically adjusting the specific authentication steps performed according to the adaptive risk.
- **Authenticator** – Something that a Subject possesses and controls (typically a cryptographic module or password) that is used to authenticate the Subject's identity. Authenticators are used to prove, with the specified Level of Assurance, that a credential is referring to the same Subject that was originally bound to the credential (e.g., password, Q&A, or one-time passcode (OTP). Note: Referred to as a token in ITSP.30.031 Glossary.
- **Credential** – An object or data structure that authoritatively binds an identity (or additional attributes) to an authenticator (also referred to as token) possessed and controlled by a Subject. A credential includes one or more identifiers which may be pseudonymous, and may contain attributes verified by the credential issuer. Note: Based on ITSP.30.031 Glossary.

1.5 Roles

The following roles are defined to cover the scope of the Notice and Consent Conformance Criteria. Depending on the use case, different organizations may take on one or more roles.

- **Subject –** in the context of Verified Login, a Subject may be a natural person, an organization, an application, or a device bound to a credential.
- **Credential Service Provider –** an entity that operates a service that implements the Verified Login Trusted Processes. (For uses cases where the private sector is delivering service capabilities to the public sector, this is a private sector entity.)
- **Relying Party –** in the context of Verified Login, an entity that depends on a conforming implementation of the Verified Login Trusted Processes. (For use cases where the private sector is delivering service capabilities to the public sector, this is a public sector activity, service or program.)

These roles help to isolate the different functions and responsibilities within the end-to-end Verified Login processes. They are not intended to imply any particular solution, architecture or implementation.

2 Trusted Processes and Conformance Criteria

2.1 Trusted Processes

The Verified Login Profile Conformance Profile defines conformance criteria as essential requirements for the Trusted Processes defined in the Verified Login Component Overview, which are:

1. **Credential Issuance –** a process during which a credential is created and bound to one or more authenticators controlled by a Subject.
2. **Authentication –** the process that establishes the confidence, or Level of Assurance, that a Subject has control over their issued credential and that the credential is currently valid (i.e., not suspended or revoked).
3. **Authentication Session Initiation –** a process that enables a persistent interaction between a Subject and an end-point, such as a Credential Service Provider or Relying Party, while removing the need to continuously repeat the authentication process between interactions.
4. **Authentication Session Termination –** an explicit logout event, session expiration due to inactivity or maximum duration, or other means.
5. **Credential Suspension –** a process that transitions an issued credential to an inaccessible credential.
6. **Credential Recovery –** a process that provides a means to transition an inaccessible credential to a usable state.
7. **Credential Maintenance –** a process that provides credential life-cycle activities such as binding new authenticators (e.g., binding a new hard OTP token), removing authenticators (e.g., removing a previously registered software OTP), and updating authenticators (e.g., password change, updating security questions and answers).
8. **Credential Revocation –** a process to render a credential as no longer usable.

A full description of the trusted processes can be found in the Verified Login Component Overview document.

2.2 Levels of Assurance

The Conformance Criteria are profiled in terms of levels of assurance. A level of assurance reflects the relative stringency of the Conformance Criteria and is used to convey a relative degree of confidence which may be accepted for use by a Relying Party. Table 1 lists the four levels of assurance defined in existing trust frameworks.

Level of Assurance	Qualification Description
Level 1 (LOA1)	• Little to no degree of confidence required • Satisfies Level 1 Conformance Criteria

184-c	Level 2 (LOA2)	• Some (reasonable) degree of confidence required • Satisfies Level 2 Conformance Criteria
184-d	Level 3 (LOA3)	• High degree of confidence required • Satisfies Level 3 Conformance Criteria
184-e	Level 4 (LOA4)	• Very high degree of confidence required • Satisfies Level 4 Conformance Criteria

185 **Table 1. Levels of Assurance**

186 2.3 Verified Login Conformance Criteria

187 Conformance criteria are organized by the Trusted Processes defined in the Verified Login
188 Component and profiled against assurance levels[1]. Within each category, conformance criteria
189 are then grouped by topics. For ease of reference, a specific conformance criteria may be
190 referred to by its category and reference no. (e.g., "**BASE-1**" refers to "Baseline Conformance
191 Criteria Reference No. 1").

192 ***Please Note**: Notification criteria specified in this conformance criteria represent only those*
193 *notifications specific to credential activities within the context of Verified Login. It is likely that*
194 *future notification criteria, along with all baseline requirements, will move to a separate*
195 *conformance profile such as Trusted Infrastructure. If that occurs, those specific criteria will be*
196 *moved as appropriate and Verified Login revised accordingly.*

197	Reference	Conformance Criteria	Level of Assurance			
198	**BASE**	**Baseline**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
199	**EVENT LOGGING**					
200	1	Credential management and use events **MAY** be logged and **MAY** be retained for a predefined period of time as evidence.	Y			
201	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	
202	3	In addition to the LOA2 requirements, the logs **MUST** have a tamper-detection mechanism to detect unauthorized modifications.			Y	
203	4	Personal information and authenticator secrets (e.g., passwords, OTP values, or security questions) **MUST NOT** be logged within the service.	Y	Y	Y	
204	**INFORMATION SECURITY**					

205	5	The Credential Service Provider **MAY** adhere to a set of Information Security Guidelines and Security Controls to protect the integrity, confidentiality, and availability of the service (e.g., CSEC ITSG-33).	Y			
206	6	The Credential Service Provider **MUST** adhere to a set of Information Security Guidelines and Security Controls to protect the integrity, confidentiality, and availability of the service (e.g., CSEC ITSG-33). The Credential Service Provider **MUST** have an auditable process to demonstrate adherence.		Y		
207	7	In addition to the LOA2 requirements, the Credential Service Provider **MUST** have an independently audited process to demonstrate adherence.			Y	
208	**IT SERVICE MANAGEMENT**					
209	8	The Credential Service Provider **SHOULD** have a documented service management practice for all aspects of the service.	Y			
210	9	The Credential Service Provider **MUST** have a documented and auditable service management practice for all aspects of the service.		Y		
211	10	The Credential Service Provider **MUST** have a documented and independently audited service management practice for all aspects of the service.			Y	
212	11	The Credential Service Provider **SHOULD** adhere to an industry standard service management framework such as Information Technology Infrastructure Library (ITIL).	Y	Y		
213	12	The Credential Service Provider **MUST** adhere to an industry standard service management framework such as ITIL.			Y	
214	**MONITORING**					
215	13	The Credential Service Provider **SHOULD** have the ability to monitor the service for indications of credential misuse or compromise.	Y			
216	14	The Credential Service Provider **MUST** have real-time monitoring of the service for indications of credential misuse or compromise.		Y	Y	
217	15	The Credential Service Provider **SHOULD** take measures to detect the misuse of the credential.	Y			
218	16	The Credential Service Provider **MUST** take measures to detect the misuse of a credential.		Y	Y	
219	**PRIVACY**					

220	17	The Credential Service Provider **MUST** adhere to the privacy risk management practices of the Trust Framework and any selected Conformance Profiles.		Y	Y	
221	18	The Credential Service Provider **MUST** adhere to the privacy risk management practices of the Relying Parties.		Y	Y	
222	19	The Credential Service Provider **MUST** adhere to applicable privacy laws and regulations for the jurisdictions in which their services operate.	Y	Y	Y	
223	**NOTIFICATIONS**					
224	20	The Credential Service Provider **MAY** notify the Subject of any changes to credential information (e.g., password update, adding or removing authenticators).	Y			
225	21	The Credential Service Provider **SHOULD** notify the Subject of any changes to credential information (e.g., password update, adding or removing authenticators).		Y		
226	22	The Credential Service Provider **MUST** notify the Subject of any changes to credential information (e.g., password update, adding or removing authenticators).			Y	
227	**CDIS**	**Credential Issuance**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
228	**BINDING A SUBJECT**					
229	1	The Credential Service Provider **SHOULD** enforce that the credential is only bound to one Subject.	Y			
230	2	The Credential Service Provider **MUST** enforce that the credential is only bound to one Subject.		Y	Y	
231	**BINDING AUTHENTICATORS**					
232	3	The Credential Service Provider **MAY** provide the ability to bind to a Subject-provided authenticator.	Y	Y	Y	
233	4	At least one authenticator (e.g., password, Q&A, or OTP) **MUST** be bound to the credential.	Y	Y	Y	
234	5	At least two different authenticators **SHOULD** be bound to the credential to recover from loss or theft of the primary authenticator.		Y		
235	6	At least two different authenticators **MUST** be bound to the credential to recover from loss or theft of the primary authenticator.			Y	

236	7	Additional authenticators, which could be used for recovery purposes, **MUST** be the same or higher LOA as the primary authenticator		Y	Y	
237	**AUTHENTICATOR CREATION**					
238	8	When the authenticator is created (e.g., hardware OTP device OR software OTP), the creator **MUST** have an auditable quality management process.		Y		
239	9	When the authenticator is created (e.g., hardware OTP device OR software OTP), the creator **MUST** have an independently audited quality management process.			Y	
240	10	When the authenticator uses information embedded by a manufacturer (e.g., hardware OTP device OR software OTP), the manufacturer **MUST** have an auditable security management process that protects that information from compromise beginning from manufacture time through delivery to the authenticator verifier.		Y		
241	11	When the authenticator uses information embedded by a manufacturer (e.g., hardware OTP device OR software OTP), the manufacturer **MUST** have an independently audited security management process that protects that information from compromise beginning from manufacture time through delivery to the authenticator verifier.			Y	
242	**CREDENTIAL STORAGE**					
243	12	The Credential Service Provider **SHOULD** enforce access controls to prevent unauthorized access to the credential information.	Y			
244	13	The Credential Service Provider **MUST** enforce access controls to prevent unauthorized access to the credential information.		Y	Y	
245	14	Any secrets bound to the credential **MUST** be either stored as a salted hash, or stored encrypted.		Y	Y	
246	15	Any credential attributes containing personal information that are stored within the service **MUST** be secured, for example, encrypted and/or hashed.	Y	Y	Y	
247	16	Backups of credential information **MUST** be encrypted prior to being transferred to long term storage.		Y	Y	
248	17	The cryptographic modules must meet an industry recognized validation standard (e.g.,FIPS 140-2).			Y	

	CRAU	Credential Authentication	Level 1	Level 2	Level 3	Level 4
AUTHENTICATORS						
1		The Credential Service Provider **MUST** require at least a single authenticator to be bound to a credential.	Y	Y		
2		If only a single authenticator is required, it **MUST** provide either a "something the Subject knows" or a "something the Subject has" authentication factor. Authenticators providing a "something the Subject is or does" authentication factor **MUST** only be used as a second authenticator.		Y		
3		The Credential Service Provider **MUST** require at least two different authenticators, providing different authentication factors, that are not susceptible to the same threat vectors.			Y	
4		One of the authenticators **MUST** be provide a "something the Subject has" authentication factor. The other authenticator **MAY** provide either a "something the Subject knows" or a "something the Subject is or does" authentication factor.			Y	
AUTHENTICATOR TYPE						
6		Any authenticator type is acceptable.	Y			
7		The Credential Service Provider **MUST** utilize industry standard or industry best practice for authentication, such as standards developed and approved by Kantara, W3C, IETF or FIDO.		Y	Y	
8		The Credential Service Provider **MUST** use authenticator types that are resistant to the threats listed in **CRAU11**.			Y	
THREAT MITIGATION						
9		The Credential Service Provider **MUST** be capable of mitigating a minimum of authenticator secret guessing and replay attacks. This **MAY** be included in the scope of the guidelines described in **BASE5.**	Y			

261	10	The Credential Service Provider **MUST** be capable of mitigating a minimum of authenticator secret guessing, replay, eavesdropping, and session hijacking. This **MUST** be included in the scope of the auditable process described in **BASE6**.		Y		
262	11	The Credential Service Provider **MUST** be capable of mitigating a minimum of 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	
263	**ADAPTIVE RISK**					
264	12	The Credential Service Provider **MAY** provide the ability to perform adaptive risk authentication.	Y			
265	13	The Credential Service Provider **SHOULD** provide the ability to perform adaptive risk authentication.		Y		
266	14	The Credential Service Provider **MUST** provide the ability to perform adaptive risk authentication unless the strongest levels of authentication are always employed for the service in question.			Y	
267	**CRYPTOGRAPHIC MODULE**					
268	15	Any cryptographic modules used in client-side authentication must meet an industry recognized validation standard (e.g., FIPS 140-2).			Y	
269	**AUTHENTICATION RESULT**					
270	16	The Credential Service Provider **MUST** return a success only when the Subject has successfully completed their authentication attempt.	Y	Y	Y	
271	17	The Credential 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	
272	18	The Credential Service Provider **MUST** digitally sign and encrypt the authentication result for the intended Relying Party.		Y	Y	
273	19	The authentication result **MUST** be valid for a specified period of time.		Y	Y	
274	**INSE**	**Initiate Session**	**Level 1**	**Level 2**	**Level 3**	**Level 4**

INITIATE SESSION						
1	The Credential Service Provider **SHOULD** provide the ability to maintain a session binding with all Relying Parties.	Y			
2	The Credential 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 Credential Service Provider **SHOULD** require the Subject to re-authenticate after a predefined period of time or event, for example when a single sign-on attempt is made to another Relying Party in the federation.	Y			
6	The Credential Service Provider **MUST** require the Subject to re-authenticate after a predefined period of time or event, for example when a single sign-on attempt is made to another Relying Party in the federation or when a Relying Party requests re-authentication.		Y	Y	
7	The Credential 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	**Terminate Session**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
SESSION TIMEOUT						
1	The Credential 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 Credential 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	

290	3	Session timeout values at LOA3 **SHOULD** be shorter than those for LOA2.			Y	
291	4	A session timeout at LOA3, **MAY** result in either a session termination, or a downgrade to an LOA2 session			Y	
292	5	In the case of a downgrade: • the Credential Service Provider **MUST** notify all Relying Parties associated to the LOA3 session; and • the session timeouts **MAY** be extended to their LOA2 values (minus the time which has already passed).			Y	
293	**TERMINATE SESSION**					
294	6	The Credential Service Provider **SHOULD** notify all Relying Parties that the session has been terminated.	Y			
295	7	The Credential Service Provider **MUST** notify all Relying Parties that the session has been terminated.		Y	Y	
296	**CRSP**	**Credential Suspension**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
297	**SUBJECT INITIATED**					
298	1	The Credential Service Provider **MAY** provide the ability for a Subject to suspend the use of or revoke its credential.	Y			
299	2	The Credential Service Provider **SHOULD** provide the ability for a Subject to suspend the use of or revoke its credential.		Y	Y	
300	**HUMAN INITIATED**					
301	3	The Credential Service Provider **MAY** provide the ability for authorized personnel to suspend the use of or revoke a credential.	Y	Y	Y	
302	4	The Credential Service Provider **SHOULD** enforce access controls to ensure only authorized personnel have access to this process.	Y			
303	5	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.		Y	Y	
304	6	In addition to LOA2 requirements, the Credential Service Provider **MUST** require authorized personnel provide an LOA3 or higher credential.			Y	
305	**SYSTEM INITIATED**					

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 an 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 an LOA equivalent to that of the credential being recovered.		Y	Y	
HUMAN INITIATED					
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 LOA2 requirements, the Credential Service Provider **MUST** require authorized personnel provide an LOA3 or higher 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			
10	The Credential Service Provider **MUST** 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	
CRMA	**Credential Maintenance**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
SUBJECT INITIATED					

322	1	The Credential Service Provider **SHOULD** provide the ability to update the authenticators bound to the credential where possible (e.g., password update, bind a new authenticator, etc.).	Y			
323	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			
324	3	The Credential Service Provider **MUST** provide the ability to update the authenticators bound to the credential where possible (e.g., password update, bind a new authenticator, etc.)		Y	Y	
325	4	The Credential Service Provider **MUST** provide the ability to allow the credential attributes (e.g., password, Q&A, recovery codes) to be modified.		Y	Y	
326	5	The Credential Service Provider **MUST** require authentication at an LOA equivalent or greater than the LOA of the credential attribute being modified (e.g., a Subject logged using a single-factor password should not be able to modify recovery codes, OTP values)		Y	Y	
327	**HUMAN INITIATED**					
328	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 reset).	Y	Y	Y	
329	7	The Credential Service Provider **MAY** provide the ability to allow authorized personnel to update the credential attributes.	Y	Y	Y	
330	8	The Credential Service Provider **SHOULD** enforce access controls to ensure only authorized personnel have access to this process.	Y			
331	9	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.		Y	Y	
332	10	In addition to LOA2 requirements, the Credential Service Provider **MUST** require authorized personnel provide an LOA3 or higher credential.			Y	
333	11	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			

12	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					
13	The Credential Service Provider **SHOULD** enforce authenticator complexity requirements and periodic authenticator refresh (e.g., Q&A complexity requirements, password updates, OTP updates).	Y			
14	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 user to revoke their own credential.	Y			
2	The Credential Service Provider **MUST** allow a user 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 **SHOULD** enforce access controls to ensure only authorized personnel have access to this process.	Y			
5	The Credential Service Provider **MUST** have the ability to allow authorized personnel to revoke a credential.		Y	Y	
6	The Credential Service Provider **MUST** enforce access controls to ensure only authorized personnel have access to this process.		Y	Y	
7	In addition to LOA2 requirements, the Credential Service Provider **MUST** require authorized personnel provide an LOA3 or higher credential.			Y	

Table 2. Verified Login Conformance Criteria

Footnotes

[1] Assurance Level 4 profile is currently out of scope, but will be completed in the near future.