PCTF Digital Wallet Conformance Profile

Document Status: Draft Recommendation V1.0

In accordance with the DIACC Operating Procedures, Draft Recommendations are a deliverable which is used to share early findings and to gather broad feedback.

This document has been developed by DIACC's Trust Framework Expert Committee. 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.

25
26
27

Table of Contents

37

38

39

40

41

42

43

44

45

46

47

1. Introduction to the PCTF Digital Wallet Conformance Criteria

This document specifies the conformance criteria for the Digital Wallet Profile of the Pan-Canadian Trust Framework (PCTF). Conformance Criteria are central to the trust framework because they specify the essential requirements agreed to by trust framework participants to ensure the integrity of their processes. This integrity is paramount because the output or result of a trusted process may be relied upon by many participants across organizational, jurisdictional and sectoral boundaries.

The PCTF Conformance Criteria are intended to complement existing privacy legislation and regulations.

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.

The Digital Wallet Profile has been described in the PCTF Digital Wallet Component Overview document. A Digital Identity Wallet is a tool a Person can use to create and manage their own identities, collect “Verifiable Credentials (VCs)” from trusted entities asserting who they are and what entitlements they have, and then control whether and how they present these VCs to relying parties.

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

The Digital Identity Wallet Profile partially overlaps with some of PCTF’s components, notably the Authentication, Notice and Consent, and Credentials components. While there is overlap with other PCTF components, the Conformance Criteria within is intended to address the full scope of establishing a trusted Digital Identity Wallet.

This Profile is organized by the trusted processes which are required for a trustworthy Digital Identity Wallet. The integrity of a Trusted Process is paramount because many Participants may rely on the output of the process, often across jurisdictional, organizational, and sectoral boundaries, and over the short-term and long-term. A process is considered to be a Trusted Process when it is assessed and certified as conforming to this Conformance Criteria.

This document includes discussion and details about Risk considerations for Digital Wallet conformance. As an entity looks to demonstrate conformance with this

framework there should be consideration for the Relying Party's risk tolerance and that risk controls are consistently implemented in a manner that is not too lenient or stringent.

The Conformance Criteria are a series of statements and requirements that will provide the foundational considerations for the entity looking to assess their digital Wallet. These conformance criteria statements form the basis of assessment for all components of the Pan Canadian Trust Framework.

Once an entity completes the conformance review and satisfies the assessment activity for all conformance criteria they will be considered compliant with the PCTF Digital Wallet Component framework. To receive the DIACC Verified by Viola certificate the participant needs to complete the assessment for the core components of the framework. (note: this language in this paragraph needs to be verified but the intention is to outline what happens when a participant completes the assessment)

The PCTF Digital Wallet Profile defines the following trusted processes in 3 broad categories:

1.1.1 Wallet Instantiation and Security Processes

1. Create Digital Wallet
2. Register Digital Wallet
3. Authentication

1.1.2 Credential Management and Use Processes

1. Request Verifiable Credential
2. Store Verifiable Credential
3. Manage Verifiable Credential
4. Display Verifiable Credential
5. Render Verifiable Credential
6. Present Proof

1.1.3 Consent Management Processes

1. Express Consent

1.2 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. The rationale for not adhering to a criterion should be documented in cases where Conformance Criteria are not adhered to.
- **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.

2. Levels of Assurance

It is essential that *Participants* in a digital ecosystem have a way to evaluate the robustness and trustworthiness of transactions within that ecosystem. In order to do so, *Participants* must share a common vocabulary that describes the level of confidence they can associate with an *Entity* or transaction, as well as a common way in which to determine that level of confidence.

In the Pan-Canadian Trust Framework™ (PCTF), a *Level of Assurance* (LoA) represents the level of confidence an *Entity* may place in the processes and other conformance criteria defined in any given component of the PCTF. *Levels of Assurance* are elemental in creating networks of trust. Levels of Assurance models only work if all *Participants* in a digital ecosystem are able to interpret them consistently. It is therefore critical that all *Participants* in an ecosystem agree upon a minimum set of criteria for each *Level of Assurance*. Only then will a *Relying Party* in that ecosystem be able to properly evaluate the risks inherent in a relationship or transaction, and the *Level of Assurance* that can be placed in *Participants*, *Credentials*, and those transactions. The components of the PCTF describe the detailed conformance criteria that should be used to evaluate such *Levels of Assurance* in the context of a given PCTF component.

For the most up to date guidance regarding Levels of Assurance, please reference the PCTF Assurance Maturity Model Draft Recommendation V1.0.

3. Digital Wallet Risks

Digital Wallets provide an important role in the foundation for trust in a digital ecosystem. In addition to any Privacy Impact Assessments an Entity might perform, it is important that Organizations participating in a trust ecosystem understand the risks that exist with the use of Digital Wallets. Figure 3 contains an illustrative table of risks to Digital Wallets and examples of mitigation strategies.

Type of Risk	Threat category	Threat scenario / Vulnerability	Additional info	Threat Agent	Impact	Proposed safeguards (e.g., input to conformance requirements)
Infosec / wallet security → harm to Holder	Wallet product quality risk.	Wallet contains software vulnerabilities that can be exploited by a malicious actor.	Accidental or malicious intent.	Hacker / attacker	Harm to ecosystem participants - trust in ecosystem; reputational risk of ecosystem as a whole and to trustmark if it has a trustmark. Harm to Holder: • Identity theft • Financial harm • Loss of privilege / access / use • Reputational harm	Wallet undergoes certification process and has trust mark proving implementer follows acceptable product development process throughout entire wallet lifecycle: • R&D / launch of wallet product • Use (includes instantiation / personalization of wallet by Holder) • Sunset • Considerations for supply chain integrity validation, security in the SDLC, 3rd party security assessments, vulnerability management process. • Speaks to need for ongoing assessment / certification.
Infosec / wallet lifecycle management → user inconvenience	Wallet product quality risk.	Wallet is no longer supported and is obsolete.		N/A	Holder is unable to perform required transactions.	• Holder acquires another Wallet that also complies with industry standards as proved by trust mark. • [Consider] Wallet represented in trust registries (e.g., DIACC list of certified wallets).

154c							• Holder chooses wallet from trusted registry.
							• Wallet undergoes certification process and has trust mark proving implementer follows acceptable product development process throughout entire wallet lifecycle:
							  ○ R&D / launch of wallet product
							  ○ use (includes instantiation / personalization of wallet by Holder)
							  ○ Sunset
							• Considerations for supply chain integrity validation, security in the SDLC, 3rd party security assessments, vulnerability management process.
							• Speaks to need for ongoing assessment / certification.
							Note: not sure how the wallet could notify the user something is wrong

154d	Infosec / wallet lifecycle management → user inconvenience	Wallet product quality risk.	Wallet is no longer supported and is obsolete.	Wallet is unable to interoperate with an Issuer or Verifier needed by the Holder.	N/A	Holder is unable to perform required transactions.	• [Consider] Wallet represented in trust registries (e.g., DIACC list of certified wallets). • Holder chooses wallet from trusted registry. • Holder acquires another Wallet that also complies with industry standards as proved by trust mark.
154e	Infosec / wallet security → harm to Holder	Wallet product quality risk.	Malicious actors develop Wallet with intent to harm Holder or impersonate	Malicious actors place wallet in Apple and Google app stores.	Malicious wallet developer.	• Phishing. • Impersonate or otherwise harm to Holder.	• Holder can identify and authenticate a certified Wallet. • Speaks to need for registries for user to

			Holder.				check certification.
154f	Infosec / wallet lifecycle management → user inconvenience.	Wallet product quality risk.	Wallet does not implement / conform industry standards.	Wallet is unable to interoperate with an Issuer or Verifier needed by the Holder.	Wallet developer.	• Denial of Service to the Holder. • Holder is unable to perform required transactions. • Issuer unable to issue. • Verifier not able to engage in a transaction with the Holder.	• Wallet implements industry standards as proved by trust mark. • Trust mark needs to ensure requirements for compliance to industry standards. • Wallet must conform / implement relevant industry standards (e.g., W3C Verifiable Credentials, DIF, DID, Governance Framework, etc.).
154g	Infosec / Issuer/Verifier security → harm to Holder.	Issuer/Verifier product quality risk.	Hosted / cloud platform (Issuers, Verifiers etc.) has inadequate technical security controls and Management Practices.		Hacker.	System is easily compromised, which could expose data stored within the Wallet, or allow a sophisticated attacker to issue fake documents.	• All participants in the ecosystem undergo certification process and have trust mark proving conformance to the standard. • Considerations for supply chain integrity validation, security in the SDLC, 3rd party security assessments, vulnerability management process • Speaks to need for ongoing assessment / certification
154h	Infosec / key management security → harm to Holder	Device security risks / key management risk.	Device does not support required security functions for specific/target LOA(s)	Device lacks adequate key management capability.	Malicious actor (local or remote).	Major: Compromised keys / compromised wallet / privacy breach / identity theft.	• Wallet explicitly supports devices and OS versions with adequate / evaluated key management capability. *Notes:* • *this includes key management functions & high-impact security functions managed on same device as wallet software as well as*

							• *device external to the wallet software.* • *"Adequate" (FIPS for hardware, NIST for software) will depend on LOA.*
154i	Infosec / key management security → harm to Holder	Backup/recovery risks / key management risks.	Weak backup / recovery process.	Malicious actor steals secret keys using backup / recovery mechanism.	Malicious actor (local or remote).	Major: Compromised keys / compromised wallet / privacy breach / identity theft.	• Backup and recovery processes to be defined for the corresponding LOA and assessed as part of the certification process. • Backups must have same LOA protections as the original protections.
154j	Infosec / key management security → harm to Holder	Wallet security risks / key management risks.	Wallet software does not support required security functions for specific/target LOA(s).	• Wallet software does not have adequate key manage-ment protections. • Malicious actor steals secret keys (e.g., steals key from memory, cracks white box crypto, power analysis).	Malicious actor (local or remote).	Major: Compromised keys / compromised wallet / privacy breach / identity theft.	• Wallet uses adequate/evaluated key management software and/or hardware with non-exportable keys. *Note: "adequate" (NIST for software) will depend on LOA.*
154k	Infosec / Authentication controls → harm to Holder	Unauthorized use of the wallet.	Device software does not support required security functions for specific / target LOA(s).	Device lacks adequate user authentication capability.	Non-Holder access.	ATO / privacy breach / identity theft.	Wallet prohibits specific devices and OS versions - LOA driven requirements.
	Infosec / data analytics	Data analytics in the	Sensitive information being passed	Unintentional or intentional.	Malicious actor.	• Sensitive data leakage in analytics	• If sensitive data required in analytics, ensure anonymized

154l	→ harm to Holder	wallet.	in data analytics collection.			• data. • Privacy breach / identity theft.	before being sent - including before saved to local storage in offline modes and also wallet files. • Trust mark to ensure privacy risk assessment is completed when adding / modifying data analytics - where assessment includes risk of unintended use of analytics data. • Trust mark to ensure access control requirements on access to analytics data.
154m	Infosec / wallet environment security → harm to Holder	Device security risks.	Device not updated with latest security updates.	Exploitable vulnerabilities.	• Malware • Elevated privilege • Man in the middle attack	Privacy breach / identity theft.	• Wallet to check for OS version on launch, notify holder & (depending on LOA) prevent wallet use until update is complete • Wallet prohibits specific devices and OS versions - LOA driven requirements.
154n	Infosec / wallet environment security → harm to Holder	Device security risks.	Device security features not enabled	e.g., Screen Lock	Non-Holder Access	Privacy breach / identity theft	• Wallet check for known vulnerabilities on launch, notifies holder of specific vulnerabilities and required corrective actions prior to wallet use. • LOA driven requirements.
154o	Infosec / Binding and authentication → harm to Holder	Unauthorized use of the wallet.	Person using the Wallet is not the authorized Holder.	When users share devices, this would allow others to issue assertions and share document of the authorized	• Hackers • Acquaintances • Family Members	Assertions are made on the behalf of the user without their consent.	• Include specific language in the EULA to ensure authorized users understand their responsibility. • Wallet level authentication (as opposed to / in addition

				holder without their consent.			to leveraging device auth). • Wallet / wallet authentication strong binding to the Verified Person.
154p	Privacy → user tracking	User tracking.	Verifier tracks Holder and shares with other Verifiers that can link via identifiers.	Digital wallet uses common identifiers across multiple verifiers	Invasion of privacy.	Linking of identifiers across Verifiers; user tracking; data aggregation.	• Wallet uses industry standard unique identifiers technologies.
154q	Privacy → user tracking	User tracking.	Issuer tracks Holders interactions with Verifiers or Issuers. (Issuer is broker here - federated model).	Issuer, Wallet, and Verifiers implement federation protocols (e.g., SAML).	Invasion of privacy.	Linking of identifiers by Issuer; user tracking; data aggregation	• Wallet uses industry standard self-sovereign / decentralized protocols. • Transparency - Privacy Notice to contain clear language
154r	Privacy → overshari ng	Over-sharing.	Digital Wallet does not support data minimization (e.g., Verifier asks for ZKP, Digital Wallet does not support it).	Holder provides more information to Verifier than appropriate.	• Rogue Verifier targeting user of specific digital wallets that do not offer data mini-mization capabilities. • Unintended Verifier that receives more information than it asked for/needs.	• Holder provides more information to Verifier than appropriate • Privacy breach / identity theft • Verifier privacy regulation non-compliance for receipt of data it did not have a business need for. • Inability for government Verifier use as government may not have authority to receive additional information	• Digital wallet to support data minimization capabilities (e.g., selective disclosure, ZKP).

						not asked for.	
154s	Privacy → overshari ng	Over-sharing.	Digital wallet does not fully disclose information to be shared to Verifier or allow Holder to control.	Incomplete, unclear, or ambiguous notice.	• Wallet developer (introduces threat) - wallet quality issue • Rogue Verifier targeting user of specific digital wallets that does not offer proper notice	• Holder provides more information to Verifier than they would have otherwise agreed to; Decisions being made by Verifier on that information could have negative impact to that user • Holder not able to accurately assess risk of information disclosure	• Wallet effectively discloses information to be shared to Holder and allows Holder to control. • *Is a summary sufficient? Not all data is understandable.*
154t	Comp-liance → privacy	Privacy.	Digital wallet does not conform to PCTF privacy component.		N/A	• Privacy non-compliance	Trustmark to ensure PCTF Privacy Component compliance as part of wallet certification.
154u	Access-ibility	Digital wallet use.	Wallet does not confirm to industry accessibility standards.		N/A	• Holder is unable to use Wallet due to disabilities; Subject vulnerable population to non-digital wallet processes that may carry more risk of identity theft. • Abandon-ment; reputational risk. • Lack of service; Over-sharing of	• Wallet implements industry standard accessibility capabilities.

						data.	

154v	Usability	Digital Wallet use.	Holder does not understand the wording of the Wallet.	• The wallet's instructions are not clear to the Holder.
				• Notice is unclear or ambiguous
				• Poor UX.
					N/A	• Holder uses Wallet in an unintended way that results in harm to the Holder.
						• Release of PII to unintended recipient (accidental privacy breach; phishing).
							• Wallet uses plain language and has consistent look and feel.
							• Robust wallet design: Prevent access to, or sharing from, without validating the entities information is being exchanged with.
							• For consideration:
							  ○ Should we add something about importance of usability studies to confirm above?
							  ○ This is outside of the digital wallet, but how do we handle recommendations for instances of harm (fraud reporting, accidental share reporting, other)?
							  ○ Robust key management - is this needed here - how does it help? Maybe needs callout for trusted registry confirmations instead.

154w	Infosec / data registry security → harm to Holder	Trusted Data Registry (TDR) quality.	Data Registry has inadequate security controls and management practices.	• Malicious actor inserts their public keys into data registry (not a wallet risk, but an eco-system risk).	Malicious actor.	• Users make unintentional / uninformed sharing decisions. • Privacy breach / identity theft.	• Data Registry subject to certification (initial and ongoing) process and trust mark. • Wallet authenticates Data Registry as Trusted; where, authentication implies a capability to ensure "is legitimate" (e.g., pre-configuration; TLS cert matches the DNS of the Issuer) *Note: In the case of pre-*

							configuration, expectation is that Wallet developer / service-provider actively monitors certified Data Registry list(s) for changes
154x	Infosec / data registry security → harm to Holder	Wallet quality.	Wallet uses Data Registry provided by malicious actor.	Digital wallet trusts public key of malicious actor.	Malicious actor that establishes a rogue data registry.	• Users make unintentional / uninformed sharing decisions. • Privacy breach / identity theft.	• Data Registry subject to certification (initial and ongoing) process and trust mark. • Wallet authenticates Data Registry as Trusted; where, authentication implies a capability to ensure "is legitimate" (e.g., pre-configuration; TLS cert matches the DNS of the Issuer). *Note: In the case of pre-configuration, expectation is that Wallet developer / service-provider actively monitors certified Data Registry list(s) for changes.*
154y	Accessib ility	Wallet quality.	Wallet does not support language of Holder.	e.g., Wallet does not support Mandarin Chinese.	N/A	Accessibility / addressable market limitations.	• Wallet implements multi-language support and/or adopts common symbols to convey meaning.
154z	Infosec / Authentic ation controls → harm to Holder	Eco-system trust & Repu-tation risk.	Holder interacts with malicious Issuer.	The Wallet does not: • Auth-enticate Issuer for the Holder resulting in harm to the Holder. • Effectively inform the Holder of verified identity of Issuer.	Malicious Issuer.	Privacy breach / identity theft.	• Wallet authenticates issuer and implement effective communication with Holder; where, authentication implies a capability to ensure "is legitimate" (e.g., public key of Issuer in certified Data Registry; TLS cert matches the DNS of the Issuer).

154a a	Infosec / Authentication controls → harm to Holder	Eco-system trust.	Holder interacts with a malicious Verifier.	The Wallet does not: • Authenticate Verifier for the Holder resulting in harm to the Holder. • Effectively inform Holder of verified identity of Verifier.	Malicious Verifier.	Privacy breach / identity theft.	• Wallet authenticates verifier and implement effective communication with holder; where, authentication implies a capability to ensure "is legitimate" (e.g., public key of Verifier in certified Data Registry; TLS cert matches the DNS of the Verifier).

157 **Figure 3: Digital Wallet Risks**

158 4. Conformance Criteria

159 Conformance Criteria are categorized by trust element. For ease of reference, a specific
160 conformance criterion may be referred to by its category and reference number.
161 Example: "BASE1" refers to "Baseline Conformance Criteria reference No. 1".

162 **Notes:**

163 • Baseline Conformance Criteria are also included as part of this conformance
164 profile.
165 • Conformance Criteria specified in other PCTF components will also be applicable
166 to the PCTF Credentials (Relationships & Attributes) Component under certain
167 circumstances.
168 • For the most up to date guidance regarding Levels of Assurance, please
169 reference the PCTF Assurance Maturity Model Draft Recommendation V1.0.

167a	Reference	Conformance Criteria	Assurance Level			
167b	**BASE**	**These Baseline Criteria Apply to <u>All</u> Digital Wallet Processes**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
167c	1	These 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.	X	X	X	X

167d	2	Where applicable, criteria pertaining to Credentials, Verifiable Credentials, Relationships, and/or Attributes **MUST** comply with the PCTF Credentials (Relationships and Attributes) LOA 1 conformance criteria.	X			
167e	3	Where applicable, criteria pertaining to Credentials, Verifiable Credentials, Relationships, and/or Attributes **MUST** comply with the PCTF Credentials (Relationships and Attributes) LOA 2 conformance criteria.		X		
167f	4	Where applicable, criteria pertaining to Credentials, Verifiable Credentials, Relationships, and/or Attributes **MUST** comply with the PCTF Credentials (Relationships and Attributes) LOA 3 conformance criteria.			X	
167g	5	Where applicable, criteria pertaining to Credentials, Verifiable Credentials, Relationships, and/or Attributes **MUST** comply with the PCTF Credentials (Relationships and Attributes) LOA 4 conformance criteria.				X
167h	6	Where applicable, criteria pertaining to Notice and Consent **MUST** comply with the PCTF Notice and Consent LOA 1 conformance criteria.	X			
167i	7	Where applicable, criteria pertaining to Notice and Consent **MUST** comply with the PCTF Notice and Consent LOA 2 conformance criteria.		X		
167j	8	Where applicable, criteria pertaining to Notice and Consent **MUST** comply with the PCTF Notice and Consent LOA 3 conformance criteria.			X	
167k	9	Where applicable, criteria pertaining to Notice and Consent **MUST** comply with the PCTF Notice and Consent LOA 4 conformance criteria.				X

167l	**CREA**	**Create Digital Wallet**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
167m	1	As part of the installation, the Wallet application **SHOULD** make sure it is being installed on an “up to date” and supported execution environment (e.g.: the operating system is **sufficiently** up to date and patched).	X			
167n	2	As part of the installation, the Wallet application **MUST** make sure it is being installed on an “up to date” and supported execution environment (e.g.: the operating system is **sufficiently** up to date and patched).		X	X	X
167o	3	The Wallet **SHOULD** ensure the latest version of the Wallet is installed, using a trusted source to check for release details and download.	X			
167p	4	The Wallet MUST notify and encourage the Holder to update/upgrade to the latest secure version of the Wallet. NOTE: The Wallet MAY identify the version of the Wallet to Issuers and Verifiers and as such allow them to manage their own risk associated with the use of a particular version of a Wallet.		X	X	X
167q	5	When updating its own code, the Wallet **SHOULD** ensure that the download is from a trusted source and has not been compromised during transit or installation (e.g.; via digital signatures)	X			
167r	6	The Wallet update process **MUST** be from a trusted source and ensure the update has not been compromised during transit or installation (e.g.; via digital signatures)		X	X	X

167s	7	The Wallet **SHOULD** use the most secure key storage and cryptographic processor (collectively the trusted execution environment) available on the platform hosting the Wallet (e.g., Mobile Phone, Browser…).	X	X		
167t	8	The Wallet **MUST** use appropriate key storage and cryptographic implementation (collectively the trusted execution environment) to the wallet target operating LoA.			X	X
167u	9	Using a trusted execution environment, the Wallet **SHOULD** initiate the creation of unique, diversified key.	X	X		
167v	10	Using a trusted execution environment, the Wallet **MUST** initiate the creation of unique, diversified keys.			X	X
167w	11	The Wallet **SHOULD** test any created diversified key(s).	X	X		
167x	12	The Wallet **MUST** test any created diversified key(s).			X	X
167y	13	The Wallet **SHOULD** be able to demonstrate its trustworthiness to Holder, Issuer, and Verifier.	X	X	X	X
167z	14	A mobile Wallet **SHOULD** be capable of ensuring the device upon which it is resident has not been rooted or similarly compromised, or be certified or assessed as being capable of operating safely in an environment that has been similarly compromised.	X			
167aa	15	A mobile Wallet **MUST** be capable of ensuring the device upon which it is resident has not been rooted or similarly compromised, or be certified or assessed as being capable of operating safely in an environment that has been similarly compromised.		X	X	X

167ab	16	A hosted Wallet service provider(s) **SHOULD** be capable of ensuring the environment upon which it is resident has not been rooted or similarly compromised , or be certified or assessed as being capable of operating safely in an environment that has been similarly compromised.	X			
167ac	17	A hosted Wallet service provider(s) **MUST** be capable of ensuring the environment upon which it is resident has not been rooted or similarly compromised , or be certified or assessed as being capable of operating safely in an environment that has been similarly compromised.		X	X	X
167ad	**REGI**	**Register Digital Wallet**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
167ae	1	The Wallet **SHOULD** provide a way to programmatically verify and cryptographically confirm its “trusted” status.	X			
167af	2	The Wallet provider **MUST** provide a way to protect the ongoing wallet “trusted” status.		X	X	X
167ag	3	The Wallet **MUST** enable a Verified Person or Verified Organization to uniquely and persistently identify a Wallet instance.			X	X
167ah	4	The Wallet **MAY** have mechanism that prevents un-authorized tracking of its activities across multiple Entities with which it interacts (e.g., must prevent Entities from aggregating information regarding Credentials, Subjects, Holders, or other information shared via the Wallet).	X			

167ai	5	The Wallet **SHOULD** have a mechanism that prevents un-authorized tracking of its activities across multiple Entities with which it interacts (e.g., must prevent Entities from aggregating information regarding Credentials, Subjects, Holders, or other information shared via the Wallet).		X		
167aj	6	The Wallet **MUST** have a mechanism that prevents un-authorized tracking of its activities across multiple Entities with which it interacts (e.g., must prevent Entities from aggregating information regarding Credentials, Subjects, Holders, or other information shared via the Wallet).			X	X
167ak	7	The Wallet **SHOULD** maintain a list of Entities with which the Wallet is registered.	X	X	X	X
167al	8	The Wallet **SHOULD** offer the Holder to de-register itself from any Entity with which it has registered.	X	X		
167am	**AUTH**	**Authentication**	**LOA1**	**LOA3**	**LOA3**	**LOA4**
167an	1	The Wallet **MUST** authenticate the holder in accordance with the PCTF Authentication component's conformance criteria for LOA1.	X			
167ao	2	The Wallet **MUST** authenticate the holder in accordance with the PCTF Authentication component's conformance criteria for LOA2.		X		
167ap	3	The Wallet **MUST** authenticate the holder in accordance with the PCTF Authentication component's conformance criteria for LOA3.			X	
167aq	4	The Wallet **MUST** authenticate the holder in accordance with the PCTF Authentication component's conformance criteria for LOA4.				X

167ar	5	The Wallet **SHOULD** challenge the Holder to Authenticate when performing actions that share, change, add, or delete personally identifiable information.	X			
167as	6	The Wallet **MUST** challenge the Holder to Authenticate to the required LoA when performing actions that share, change, add, or delete personally identifiable information.		X	X	X
167at	7	The Wallet **SHOULD** store Credentials and private keys in secure storage. NOTE: Please refer to the Authentication Credential Storage section of the Authentication component - CDIS 17 - 21.	X	X		
167au	8	The Wallet **MUST** store Credentials and private keys in secure storage. NOTE: Please refer to the Authentication Credential Storage section of the Authentication component - CDIS 17 - 21.			X	X
167av	9	The Wallet **SHOULD** record and securely store information (e.g., time, date, user identification) regarding authentication events. The Wallet must conform to PCTF Authentication component conformance criteria 1 and 5.	X			
167aw	10	The Wallet **MUST** record and securely store information (e.g., time, date, user identifier) regarding authentication events. The Wallet must conform to PCTF Authentication component conformance criteria 2, 3, 4, and 5.		X	X	X
167ax	**REQU**	**Request Verifiable Credential**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
167ay	1	The Wallet **MAY** provide a list of supported Verified Issuer Organizations and/or networks or trust ecosystems within which it is capable of operating.	X	X	X	X

167az	3	The Wallet **MAY** allow a user to initiate the request Verifiable Credential flow.	X	X	X	X
167ba	4	The Wallet **MAY** support requesting one or more attributes from an Entity.	X	X	X	X
167bb	5	The Wallet **MAY** support requesting one or more attributes of a Verifiable Credential from another Holder.	X	X	X	X
167bc	6	The Wallet **MAY** allow the user to check the status of a Verifiable Credential request.	X	X	X	X
167bd	7	The Wallet **SHOULD** retain a history of Verifiable Credential requests.	X	X	X	X
167be	**STOR**	**Store Verifiable Credential**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
167bf	1	The Wallet **SHOULD** provide a secure storage capability that conforms to currently accepted standards and best practices for secure storage (e.g., currently accepted best practices for encryption).	X			
167bg	2	The Wallet **MUST** provide a secure storage capability that conforms to currently accepted standards and best practices for secure storage (e.g., currently accepted Canadian standards for encryption).		X	X	X
167bh	3	The Wallet **MAY** store the storage encryption key in local storage.	X	X		
167bi	4	The Wallet **SHOULD** access the storage encryption key using strong authentication.	X			
167bj	5	The Wallet **MUST** access the storage encryption key using strong authentication.		X	X	X
167bk	6	The Wallet **SHOULD** provide multi-factor authentication options for Holders accessing secure storage.	X			

167bl	7	The Wallet **MUST** provide multi-factor authentication options for Holders accessing secure storage.		X	X	X
167bm	8	The Wallet **MAY** require multi-factor authentication for Holders accessing secure storage.	X	X		
167bn	9	The Wallet **SHOULD** require multi-factor authentication for Holders accessing secure storage.			X	X
167bo	**MANA**	**Manage Verifiable Credential**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
167bp	1	The Wallet **SHOULD** support displaying all attributes of a Verifiable Credential.	X			
167bq	2	The Wallet **MUST** support displaying all attributes of a Verifiable Credential.		X	X	X
167br	3	The Wallet **MUST** allow the Holder to delete Credentials from the Wallet.	X	X	X	X
167bs	4	The Wallet **SHOULD** record Credential management events in an audit log. The Wallet must conform to PCTF Authentication component conformance criteria 1 and 5.	X			
167bt	5	The Wallet **MUST** record Credential management events in an audit log. The Wallet must conform to PCTF Authentication component conformance criteria 2, 3, 4, and 5.		X	X	X
167bu	6	The Wallet **SHOULD** record Credential management events in an audit log stored in a secure storage area.			X	X
167bv	7	The Wallet **SHOULD** indicate to the Holder the current status of Credentials (e.g., whether the Credential has expired or has been revoked).	X			
167bw	8	The Wallet **MUST** indicate to the Holder the current status of Credentials (e.g., whether the Credential has expired or has been revoked).		X	X	X

167bx	9	The Wallet **SHOULD** allow the Holder to request revocation of a Credential.	X	X	X	X
167by	**DISP**	**Display Verifiable Credentials**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
167bz	1	The Wallet **MUST** enable the Holder to browse a list of all Credentials stored within it and display the details of any Credential selected by a Holder.	X	X	X	X
167ca	2	The Wallet **MUST** be enable its Holder to select a specific Credential and display its details and Attributes.	X	X	X	X
167cb	3	The Wallet **MAY** record that an Holder has displayed a Credential or Credentials and which Credential or Credentials have been displayed and when.	X	X	X	
167cc	4	The Wallet **SHOULD** record that an Holder has displayed a Credential or Credentials and which Credential or Credentials have been displayed and when.				X
167cd	5	The Wallet **SHOULD** implement best practices for the prevention of unintentional or malicious screen recording while displaying Credential Attributes or details.	X	X		
167ce	**REND**	**Render Verifiable Credential**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
167cf	1	The Wallet **SHOULD** support accessibility standards when rendering Credentials.	X	X	X	X
167cg	2	The Wallet **SHOULD** provide the holder with the ability to reveal or mask specific Attributes.	X	X	X	X
167ch	3	The Wallet **SHOULD** provide the holder with the ability to render Credentials in a human recognizable format.	X	X	X	X
167ci	4	The Wallet **SHOULD** support localization in rendering the Credential.	X	X	X	X

167cj	**PRES**	**Present Proof**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
167ck	1	The Wallet **MUST** request permission from the Wallet holder to present a proof when requested.	X	X	X	X
167cl	2	The Wallet **MUST** display the requested attributes for a proof request.	X	X	X	X
167cm	3	The Wallet **MUST** allow the Holder to authorize zero or more proofs to be sent when more than one proof is requested by an Entity in a single request.	X	X	X	X
167cn	4	The Wallet **MAY** allow the Holder to select which Attributes are provided in a proof before it is sent to the requester.	X	X	X	X
167co	5	The Wallet **SHOULD** allow an Holder to present a proof without an explicit proof request.	X	X	X	X
167cp	6	The Wallet **SHOULD** allow selective disclosure of proof attributes from any Credential.	X	X	X	X
167cq	7	The Wallet **SHOULD** support zero knowledge proofs and Derived Predicates.	X	X	X	X
167cr	8	The Wallet's Holder **SHOULD** be notified of proof requests.	X			
167cs	9	The Wallet **MUST** record all proof requests.	X	X	X	X
167ct	10	The Wallet **MAY** allow the Holder to establish pre-request approval or rejection of requests of a specific proof from a specific Entities.	X	X	X	
167cu	11	The Wallet **SHOULD** retain a history of proof requests for a predetermined period of time appropriate to the implementation. This period must be communicated with the Holder in advance of their use of the wallet.	X	X		

167cv	12	The Wallet **MUST** retain a history of proof requests for a predetermined period of time appropriate to the implementation. This period must be available to the Holder in advance of their use of the wallet.			X	X
167cw	13	The Wallet **SHOULD** retain a history of proof presentation.	X	X		
167cx	14	The Wallet **MUST** retain a history of proof presentation for a predetermined period of time appropriate to the implementation. This period must be available to the Holder in advance of their use of the wallet.			X	X
167cy	**EXPR**	**Express Consent**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
167cz	1	The Wallet **MUST** request consent to share information or Credentials from the Holder (i.e., the Holder) according to the criteria set forth in the PCTF Notice and Consent component.	X	X	X	X
167da	2	The Wallet **MUST** allow the Holder to approve or reject the consent request.	X	X	X	X
167db	3	The Wallet **SHOULD** record a history of consent requests, including information regarding whether approval was granted or rejected. This should be retained for a predetermined period of time appropriate to the implementation. This period must be available to the Holder in advance of their use of the wallet.	X			
167dc	4	The Wallet **MUST** retain a history of consent requests, including information regarding whether approval was granted or rejected.		X	X	X

167dd	5	Storage and/or retention of notice conditions and consent decision information **MUST** comply with the legislation and regulations of the jurisdiction(s) where the Record Consent is being applied and **MUST** comply with the conformance criteria set forth in the PCTF Notice and Consent.	X	X	X	X
167de	6	The Wallet **SHOULD** notify the consent notice requestor of a Holder's affirmative consent decision.	X			
167df	7	The Wallet **MUST** notify the consent notice requestor of a Holder's affirmative consent decision.		X	X	X

5. Revision History

Version	Date	Author(s)	Comment
0.01	01-17-2022	PCTF Digital Wallet Design Team	Initial Discussion Draft created by the PCTF Digital Wallet Design Team
0.02	02-28-2022	PCTF Digital Wallet Design Team	Updated version to incorporate TFEC feedback
1.0	03-30-2022	PCTF Digital Wallet Design Team	TFEC approves as Draft Recommendation V1.0