



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

PCTF Digital Wallet Component Overview

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](#).

This document is provided "AS IS," and no DIACC Participant makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose. Those who are seeking further information regarding DIACC governance are invited to review the [DIACC Controlling Policies](#).

IPR: [DIACC Intellectual Property Rights V1.0 PDF](#) | © 2022

25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55

Table of Contents

1. Introduction.....	3
1.1 Purpose and Anticipated Benefits.....	3
1.2 Context.....	3
1.3 Scope	5
1.3.1 Digital Wallet Types and Implementations.....	5
1.3.2 In-Scope Topics.....	6
1.3.3 Out-of-Scope Topics	7
1.4 Relationship to the Pan-Canadian Trust Framework.....	8
2. Conventions	9
2.1 Terms and Definitions	9
2.2 Abbreviations.....	13
2.3 Roles.....	13
3. Trust Relationships	14
4. Trusted Processes	16
4.1 Conceptual Overview.....	17
4.2 Process Descriptions	17
4.2.1 Wallet Instantiation and Security Processes	18
4.2.2 Credential Management and Use Processes.....	19
4.2.3 Consent Processes	21
5. References	21
6. Revision History.....	22

56 1. Introduction

57 This document provides an overview of the PCTF Digital Wallet Component, a
58 component of the [Pan-Canadian Trust Framework](#) (PCTF). For a general introduction to
59 the PCTF, please see the [PCTF Model Overview](#). The PCTF Model Overview describes
60 the PCTF's goals and objectives and provides a high-level overview of the PCTF.

61 Each PCTF component is described in two documents:

- 62 1. **Overview:** Introduces the subject matter of the component. The overview
63 provides information essential to understanding the Conformance Criteria of the
64 component. This includes definitions of key terms, concepts, and the Trusted
65 Processes that are part of the component.
- 66 2. **Conformance Profile:** Specifies the Conformance Criteria used to standardize
67 and assess trust elements that are part of this component.

68 This overview provides information related to and necessary for consistent interpretation
69 of the [PCTF Credentials \(Relationships & Attributes\) Conformance Profile](#).

70 1.1 Purpose and Anticipated Benefits

71 The purpose of this component is to provide a framework that Digital Identity Ecosystem
72 Participants can use to assess the degree to which the digital wallets that are part of
73 their respective ecosystems accomplish the following:

- 74 1. Provide Citizens and Consumers with a Digital Identity Wallet that complies with
75 the human rights principles of preserving people's privacy and control over their
76 information.
- 77 2. Introduces a consistent identity metaphor and consent-driven automated
78 experience across all Ecosystem Participants to reduce impact on users caused
79 by Digital Transformation.
- 80 3. Contribute to a stable infrastructure with longevity and world-wide interoperability
81 by adopting and supporting relevant standards as appropriate (e.g., W3C
82 Standards for Verifiable Credentials and DIDs).
- 83 4. Counter cyber vulnerability and extortion by enabling Service Providers to
84 incrementally replace existing login mechanisms, some of which may be
85 exploitable, without suffering negative impact to business.
- 86 5. Establish an environment of trust within which the wallet's owner can interact with
87 other Ecosystem Participants such as Issuers, Verifiers, and other Relying
88 Parties.

89 1.2 Context

90 The physical wallet is a private container for the owner’s cash, payment cards, proof of
91 identity, and other documents. Digital Identity Wallets are analogous to physical wallets
92 in that they contain digital versions of the Wallet Owner’s identity proofs and related
93 assets. These assets typically include digital versions of familiar physical cards and
94 documents (e.g., driver’s license, proof of insurance, health cards, etc.). Digital assets
95 are often stored as a form of credential (often a verifiable credential) – and this term is
96 used throughout this document to refer to wallet contents. A digital identity wallet may
97 also store cryptographic keys used by the wallet’s owner. They are typically small
98 software applications residing on personal computing devices.

99 A well-designed digital identity wallet ensures the security of its sensitive and
100 confidential contents while making it easy for the wallet owner to use digital identities
101 proofs and credentials in online and face to face interactions. A well-designed digital
102 identity wallet can enhance privacy by providing the wallet owner with control over and
103 visibility into when, where, how, and what wallet contents are disclosed to third parties.

104 The concept of digital identity wallets as a way for owners to store, manage, and use
105 digital identities and related assets emerged as identity systems evolved from
106 application specific user authentication mechanisms to sophisticated systems that share
107 and verify identity assets among multiple entities (applications, service providers, other
108 individuals, etc.) in various federation and trust arrangements.

109 Among the specific factors that have encouraged the emergence of digital identity
110 wallets are:

- 111 1. **Increasing concerns about privacy invasion** – Surveillance of users by
112 commercial and state actors has become visible and is now a political factor
113 driving public policy. Browser makers and software vendors have made efforts to
114 reduce opportunities to track users online. However, the use of e-mail addresses
115 and phone numbers (which are personally identifiable information) as universal
116 identifiers remains common practice. In addition, escalating numbers of email
117 and phone numbers leaked via escalating data breaches renders them unreliable
118 as identifiers and increasing the privacy with digital wallets actually makes illicit
119 use harder to track.
- 120 2. **Limitations of legacy identity solutions** – A major business consideration, if
121 not a considerable challenge, for organizations attempting to digitalize
122 an important and valuable service is minimizing the redundancy, duplication, and
123 overlap that can result as identity solutions proliferate within and between service
124 providers. As this happens, users are faced with managing multiple digital
125 identities and related assets. This is evident in the widespread use of password
126 managers to ease the burden of keeping each service relationship secure. Digital
127 identity wallets can help wallet owners manage a growing number of identity
128 assets and control the sharing and use of these assets in their digital
129 relationships and interactions.
- 130 3. **Fragmented user experience** – Service providers understandably provide users
131 digital experiences that are optimized for their own processes. Digital user

- 132 experiences seldom consider the full extent of an individual’s digital relationships
133 and interactions. The result is that many individuals are left to navigate widely
134 dissimilar and often confusing digital services. Digital identity wallets can provide
135 a trusted, consistent and familiar user experience for key aspects of interactions
136 involving digital identities (i.e., storing, retrieving, and presenting identity
137 information).
- 138 4. **Professionalization and militarization of cyber-attacks** – Fragmented user
139 experiences, the existence of numerous single purpose Digital Identities, and
140 proliferation of personal information across internet-connected systems make it
141 easy for skilled and motivated malicious actors to compromise personal
142 information and privacy. Digital Identity Wallets can help mitigate many attack
143 vectors (primarily phishing and other attacks based on obtaining personal
144 information). Moreover, Digital Identity Wallet Holders can help improve
145 overall cybersecurity by selectively sharing only the identity information needed
146 for a specific purpose or interaction (e.g., via a Zero-Knowledge proof or Derived
147 Predicate).
- 148 5. **Industry standards for verifiable credentials and personal information** – A
149 significant barrier to near real-time digital interaction is the need to revert to time-
150 consuming, labour-intensive processes for validating identities and personal
151 information. These validations are necessary to maintain process integrity for
152 high-value services but erode efficiency and user experience. Where
153 opportunities exist to automate data verification (e.g., a connection between the
154 service provider and the CRA to confirm taxable income), information security
155 and privacy mechanisms may be difficult to implement without compromising
156 user experience or contravening existing legislation. Portable, cryptographically
157 verifiable credentials, used in conjunction with digital identity wallets, are now
158 gaining acceptance as a way for service providers to obtain high assurance data
159 while ensuring security and transparency for the wallet owner. The World Wide
160 Web Consortium (W3C) Verifiable Credentials Data Model 1.0 has attracted wide
161 interest and support as the core data standard to facilitate interoperable verifiable
162 credentials.

163 **1.3 Scope**

164 Topics that are considered in and out of scope define the scope of this PCTF
165 component. Digital wallet types and their typical contents are also a key determinant of
166 component scope.

167 **1.3.1 Digital Wallet Types and Implementations**

168 The term “digital identity wallet” appears throughout this document and is an indicator of
169 this PCTF component’s scope. The focus of this component are digital wallets that
170 contain digital identities and related assets. The design of these digital wallets is such
171 that they are optimized to help the wallet owner manage and use:

- 172 1. Personal identity documents and attributes (e.g., foundational evidence of
173 identity, social insurance numbers, passports, driver's licenses, public health
174 cards, proof of citizenship, proof of residency, proof of age, etc.)
- 175 2. Personal information about and relationships with significant others (e.g., proof of
176 marital status to another individual, proof of custodianship over minors, proof of
177 employment status at an organization)
- 178 3. Encryption and signing keys to support attribute verification and digital document
179 signing

180 Digital identity wallets may also contain and facilitate use of:

- 181 1. Digital payment information (e.g., credit cards) for various services and websites
- 182 2. Authentication details (e.g., usernames/passwords) for various services and
183 websites

184 Because of this overlap with digital wallets and applications designed exclusively for
185 digital payments and financial transactions (e.g., a Bitcoin cryptocurrency wallet) certain
186 conformance criteria specified for this PCTF component may be applicable to wallets
187 and applications used exclusively for digital payments. However, this profile will not
188 explicitly address those types of wallets. Similarly, applications that function strictly as
189 password managers or form-filling utilities are not considered in scope for this PCTF
190 component.

191 The scope of this PCTF component is not limited to a particular implementation model
192 for digital identity wallets and specifies conformance criteria generally applicable to all
193 digital identity wallets, whether they are implemented as:

- 194 1. Native apps on smartphones and other mobile devices
- 195 2. Progressive web apps that execute on smartphones and laptops,
- 196 3. Traditional web hosted applications that execute on servers.

197 The scope of this PCTF component is not limited to digital identity wallets used by a
198 single individual. The scope of this component includes:

- 199 1. Digital identity wallets designed for use by individuals operating on their own
200 behalf, their family members, or for individuals that are representing a business
201 or another type of organization.
- 202 2. Organizations that require control of a corporate digital wallets that their
203 employees and representatives can use for authorized purposes.

204 **1.3.2 In-Scope Topics**

205 In scope for this PCTF component are the following topics:

- 206 1. Product and Service Quality: from a trust perspective, the software development,
207 distribution, and holder support processes used to implement and support a

- 208 digital wallet are critical aspects. Third party testing and validation of Digital
209 Wallets and the provision of trust marks can improve a digital wallets
210 trustworthiness. For progressive web apps and web hosted wallets the
211 Infrastructure (Technology & Operations) Component of the PCTF should apply
212 to these hosting services.
213 2. The following functional capabilities of digital wallets and standards are in scope:
- 214 a. Authentication of holder to open, use, and provide consent a digital wallet
215 such as mobile phone biometric and pin code authentication, multi-factor
216 authentication mechanisms, and username/password mechanisms (low
217 assurance wallets).
 - 218 b. Ability for digital wallets to authenticate Credential Issuers, Verifiers, and
219 associated verifiable data registries.
 - 220 c. Key Management technology standards for securely managing and storing
221 public/private keys, including optional ability to export, import, and
222 backup/recovery of keys.
 - 223 d. Credential Management technology standards for securely managing and
224 storing credentials held by digital wallets, including optional ability to
225 export, import, and backup/recovery of credentials, and support issuer
226 branding and policies.
 - 227 e. Ability for digital wallets to store and present attestation tokens from
228 trusted identity providers in a pre-Verifiable Credential environment
 - 229 f. Technology standards for request and provision with issuers, including
230 digital signatures.
 - 231 g. Technology standards for credential presentation with verifiers, including
232 digital signatures.
 - 233 h. Support for Minimal disclosure and zero knowledge proof technology.
 - 234 i. Holder dialog to support informed decisions to disclose or not, including
235 consent dialog.
- 236 3. Accessibility and affordability standards applicable to digital identity wallets.
237 4. Plain language and standard display format (i.e., Wallet and cards
238 representation).
239 5. Multi-Language Capability.
240 6. Informed, traceable Consent and activity/history logging and reporting.

241 **1.3.3 Out-of-Scope Topics**

242 The following topics are considered not in scope for this component:

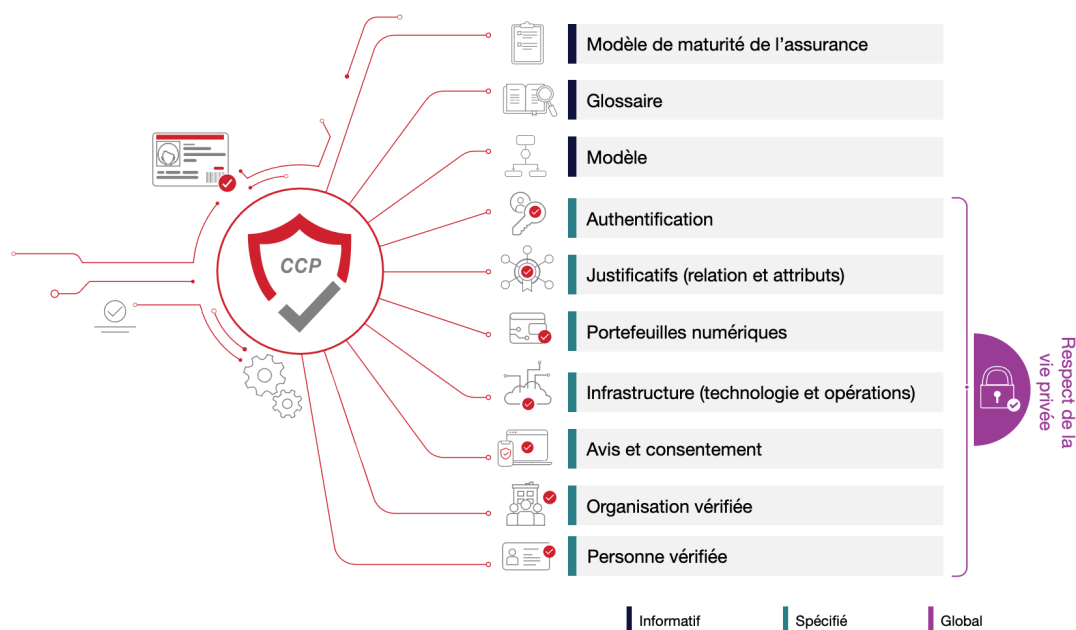
- 243 1. Technology standards, processes, and policies applicable to Credential Issuers,
244 except as directly related to wallet functionality.
- 245 2. Technology standards, processes, and policies applicable to Credential Verifiers,
246 except as directly related to wallet functionality.
- 247 3. Technology standards, processes, and policies applicable to Verifiable Data
248 Registries, except as directly related to wallet functionality.

249 1.4 Relationship to the Pan-Canadian Trust 250 Framework

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

256 **Note:** The Digital Identity Wallet component partially overlaps with the Authentication,
257 Notice and Consent, and Credentials components. As such, this PCTF component
258 represents an intersection point between several other components and expands
259 conformance criteria to include a specific tool available to participants in digital identity
260 ecosystems.

261 Figure 1 is an illustration of the components of the draft Pan-Canadian Trust
262 Framework.



263

264 Figure 1. Components of the Pan-Canadian Trust Framework

265 The Digital Identity Wallet component partially overlaps with the Authentication, Notice
266 and Consent, and Credentials components. The decentralized identity architecture, that
267 the digital identity wallet is a component of, did not exist when the PCTF structure was
268 defined and has resulted in this overlap. As the overview develops, especially with

269 respect to identification of trusted processes, this section will be updated to provide
270 required guidance on the relationship to the PCTF.

271 **2. Conventions**

272 This section describes and defines key terms and concepts used in the PCTF Digital
273 Wallet Component. This information is provided to ensure consistent use and
274 interpretation of terms appearing in this overview, and in the [PCTF Credentials](#)
275 [\(Relationships & Attributes\) Conformance Profile](#).

276 **Notes**

- 277 • Conventions may vary between PCTF components. Readers are encouraged to
278 review the conventions for each PCTF component they are reading.
- 279 • Key terms and concepts described and defined in this section, the section on
280 Trusted Processes, and the PCTF Glossary are capitalized throughout this
281 document.
- 282 • Hypertext links may be embedded in electronic versions of this document. All
283 links were accessible at time of writing.

284 **2.1 Terms and Definitions**

285 For purposes of this PCTF component, terms and definitions listed in the PCTF
286 Glossary and the terms and definitions listed in this section apply.

287 **Attestation**

288 A trusted verification of something as true or authentic

289 **Attribute**

290 An Attribute is information related to a characteristic or inherent part of an Entity (e.g.: a
291 Subject's given name or residential street address). Attributes are sometimes referred to
292 as "properties" or "claims". Attributes are stored in Credentials.

293 **Claim**

294 A Claim is an assertion made about a Subject (e.g., the Subject is licensed to drive; the
295 Subject is over 21 years of age).

296 **Credential**

297 A Credential is a set of one or more Claims made about a subject by a single Entity
298 (e.g., the Subject is licensed to drive; the Subject resides at a specified address; the

299 Subject has a specific certification). In this document the term “Credentials” does not
300 include Authentication Credentials unless the term “Authentication Credentials” is used
301 explicitly (see also, Verifiable Credential).

302 **Credential Verification**

303 Credential Verification is the evaluation of whether a Verifiable Credential or Verifiable
304 Presentation authentically represents the Issuer or Subject. This includes verification
305 that the proof is satisfied (normally via cryptographic validation), confirmation the
306 Credential or Presentation is valid (e.g., is not suspended, revoked, or expired), and that
307 the Credential or Presentation conforms to relevant specifications and/or standards.

308 **Derived Predicate (See Also: Zero Knowledge Proofs)**

309 A Derived Predicate is a Verifiable, Boolean assertion about a Subject based upon the
310 value of another Attribute that describes that Subject. For example, consider a Subject
311 who wishes to prove they are eligible for services only available to people who are at
312 least 21 years of age, and who possess a Credential which contains an Attribute that
313 holds their date of birth. Rather than present their birth date as proof they are eligible,
314 the Subject could present a Derived Predicate such as "Over21" which contains a
315 "True" or "False" value that indicates whether the Subject is greater than 21 years of
316 age. Use of Derived Predicates better protects a Subject's privacy by not releasing
317 detailed personally identifiable information while enabling a Verifier to validate a
318 Subject's eligibility for a service.

319 **Digital Identity Wallet (Wallet, Digital Wallet)**

320 A Digital Wallet is a software-based Credential Repository system that securely stores
321 information for an Owner. Depending upon the nature of the wallet, it may contain
322 information such as Credentials, Verifiable Credentials, payment information, and/or
323 passwords.

324 The purpose of a Wallet is to securely store Credentials and or Identity Attributes, and
325 to enable the Holder to assemble and prepare Verifiable Presentations. Some Wallets
326 might have identity proofing capabilities and/or Agents to facilitate the sharing of
327 Credentials they manage.

328 **Diversified Key**

329 In order to secure interactions with a population of Digital Wallets, a "key-generating
330 key" is used along with data unique to a specific instance of a Wallet to derive a diverse
331 set of keys for use with that Wallet. The data may be something unique to the instance
332 of the wallet or the device upon which it is stored. That data is often accessible to a
333 broad group, so handling of the key-generating key with a high degree of security is
334 paramount so the Wallets of that type are not compromised.

335 **Presentation**

336 A Presentation is data, typically representing one or more Claims about a Subject, that
337 is derived from one or more Credentials, Verifiable Credentials, Endorsed
338 Relationships, or Verifiable Relationships and shared with a Verifier.

339 **Relationship**

340 A Relationship is a specific type of Credential that describes the way in which two or
341 more Entities are related to each other (e.g., Fatima is a PhD student at the University
342 of British Columbia; Eric is an employee of FictitiousCorp; Sheila is a member in good
343 standing with the Law Society).

344 **Render Credential**

345 Styling the visual presentation of various entities types and data (e.g. credentials) is a
346 common need that runs across many different use cases. In order to provide a
347 predictable set of styling and data display hints to User Agents, Issuers, Verifiers, and
348 other participants who render UI associated with entities and data, this specification
349 endeavours to standardize a common data model to describe generic style and data
350 display hints that can be used across any formulation of UI elements.

351 **Repository / Credential Repository**

352 A Repository is a software-based system (application) such as a database, storage
353 vault, or Verifiable Credential Wallet that stores, and controls access to, a Holder's
354 Verifiable Credentials.

355 **Secure Storage**

356 Secure storage is a facility used to ensure stored data security, privacy and integrity.
357 This facility may rely upon the physical protection of the hardware on which the data is
358 stored, as well as security software. Data stored in secure storage either cannot be
359 retrieved from storage, or can only be retrieved by authorized parties.

360 See also <https://www.techopedia.com/definition/29701/secure-data-storage> .

361 **Selective Disclosure**

362 A Credential may contain multiple claims as key value pairs. For example, the W3C
363 proposed citizenship vocabulary includes given name, family name, gender, image and
364 birth date among other data elements in the credential schema. As a principle, data
365 minimization should be employed whenever possible to limit the sharing of personal
366 information. A data minimized proof of age to a Verifier, from the above example, might
367 only include the holders date of birth and a possibly a photo image.

368 Zero-knowledge cryptographic techniques can be employed to create a selective
369 disclosure proof based on the original credential with blinded data elements that the
370 holder does not want or need to share with a Verifier and/or Relying Party. The proof is
371 crafted in such a way that the holder can still prove to the Verifier that Credential was
372 signed by the Issuer and that the presented data was not tampered with. Common
373 signature schemes include CL signatures, BBS+ signatures and SNARK based
374 schemes.

375 One powerful use of the selective disclosure is to blind the binding identifier common to
376 a group of issued Credentials. This reduces the risk of tracking holder activity as the
377 binding secret is not disclosed to the Verifier.

378 Note: selective disclosure can be achieved via other methods such as just in time
379 issuance of credentials or using a trusted broker. These methods are not recommended
380 as all user activity is traceable to a single source – the Issuer or the broker.

381 **Token**

382 A digital representation of an attestation or container for claim(s)

383 **Verifiable Credential**

384 A Verifiable Credential is a tamper-evident Credential that is encoded in a way that
385 enables its integrity and authorship (i.e., source) to be confirmed via cryptographic
386 Verification. Verifiable Credentials must be cryptographically secure and machine
387 Verifiable.

388 **Verifiable Data Registry**

389 A role a system might perform by mediating the creation and [verification](#) of identifiers,
390 keys, and other relevant data, such as [verifiable credential](#) schemas, revocation
391 registries, issuer public keys, and so on, which might be required to use [verifiable](#)
392 [credentials](#).

393 (Reference: <https://www.w3.org/TR/vc-data-model/#dfn-verifiable-data-registries>)

394 **Verifiable Presentation**

395 A Verifiable Presentation is a tamper-evident Presentation that is encoded in a way that
396 enables its integrity and authorship (i.e., source) to be confirmed via cryptographic
397 Verification.

398 **Zero Knowledge Proofs**

399 A zero-knowledge proof is a cryptographic technique that allows the Holder to prove to
400 a Verifier that the Holder has knowledge of a value without actually sharing the value.

401 A zero-knowledge proof can be used within the context of digital identity to support the
402 following key privacy preserving features:

- 403 • Selective Disclosure – disclose a subset of attributes from a credential to an
404 issuer
- 405 • Predicates – calculations on attributes such as equality or greater than (e.g.:
406 prove your salary is greater than x or your age is greater than y) where actual
407 values are not shared with Verifier
- 408 • Signature blinding – randomization of Issuer signature prior to sharing with the
409 verifier to eliminate the signature as a correlating factor
- 410 • Private holder blinding – the correlating identifier is not exposed to the Verifier

411 **2.2 Abbreviations**

412 The following abbreviations and acronyms appear throughout this overview and the
413 [PCTF Credentials \(Relationships & Attributes\) Conformance Profile](#):

- 414 • **PCTF**: Pan-Canadian Trust Framework
- 415 • **CAL**: Credential Assurance Level
- 416 • **DiD**: Decentralized Identifier

417 **2.3 Roles**

418 The following roles and role definitions are applicable in the scope and context of the
419 [PCTF Credentials \(Relationships & Attributes\) Component](#).

420 **Notes**

- 421 • An Entity may assume one role or multiple roles, depending on the use case. For
422 example, an Entity that is the Relying Party in a transaction may also be the
423 Verifier for that transaction.
- 424 • Role definitions do not imply or require a specific solution, architecture,
425 implementation, or business model.

426 **Applicant**

427 An Applicant is any Entity that has requested, though not yet received, a Credential
428 (e.g., a Person who has requested, though not yet received, a drivers' license from a
429 province or territory). This Entity may or may not be a Subject of the Credential.

430 **Holder**

431 A Holder is any Entity that possesses one or more Credentials. The Holder is usually
432 the Subject of the Credential but need not be so (e.g., a parent might possess a

433 Credential belonging to their child; an attorney might possess a Credential on belonging
434 to their client). Holders may store Credentials they possess in a Repository.

435 **Issuer**

436 An Issuer is any Entity that makes information about a Subject available by creating and
437 issuing a Credential, Attestation Token, or Verifiable Credential (e.g., a province or
438 territory that issues a drivers' license).

439 **Relying Party**

440 A Relying Party is any Entity which consumes Digital Identity Information, Attributes,
441 Relationships, or other Credentials to conduct digital transactions (e.g., a liquor store or
442 business owner that needs to ensure a customer is old enough to purchase alcohol).
443 See Verifier below.

444 **Revocation Authority**

445 A Revocation Authority is any Entity with exclusive or primary responsibility for revoking
446 Credentials and maintaining information about revoked Credentials. The Revocation
447 Authority may be the Issuer of the revoked Credential but need not be so.

448 **Verifier**

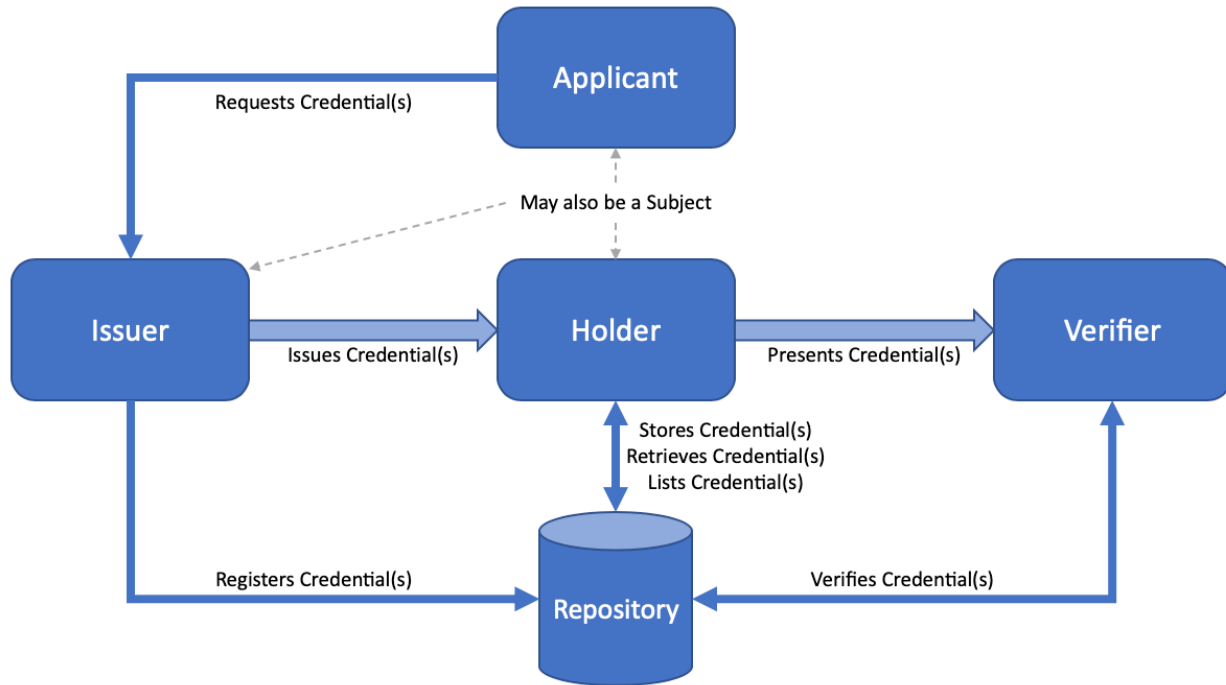
449 A Verifier is any Entity that receives one or more, Attestation Tokens, Verifiable
450 Credentials and evaluates whether the Credential(s) authentically and accurately
451 represent the Issuer or Subject (see Credential Verification). A Verifier is a Relying
452 Party that consumes and verifies Digital Identity information in the form of Attestation
453 Tokens or Verifiable Credentials.

454 **3. Trust Relationships**

455 The authenticity, validity, security, and privacy of the Entities who are involved in the
456 creation, issuance, storage, Presentation, and Verification of digital Credentials are key
457 to assessing the trustworthiness of those Credentials. This PCTF component identifies
458 key trust relationships that are factors in assessing the trustworthiness of digital
459 Credentials. In consideration of this, the Conformance Criteria associated with the trust
460 relationships and processes identified in this component focus on transparency,
461 auditability, and privacy in addition to technical methods for building trust across the
462 parties involved. Figure 2 provides some illustrative examples of how various roles
463 relate to one another and create the need for these trust relationships.

464

465



466
467

Figure 2. Digital Wallet Roles and Relationships (Illustrative)

468 It should be noted that both the W3C Verifiable Credentials Data Model, the Public
469 Sector Profile of the Pan Canadian Trust Framework, and the Hyperledger Aries project
470 include great work in this area which was taken into consideration as this component
471 was developed.

472 Trust relationships described below do not always map directly to discrete technical or
473 business processes.

474 This component advises Digital Ecosystem Participants to consider the following key
475 requirements for establishing trust in these Relationships and which affect a
476 Credential's trustworthiness:

- 477 1. Participants must be able to assess the authority and reliability of Issuers and
478 that Issuers are thorough in establishing the accuracy of information included in a
479 Credential.
- 480 2. Participants must be confident that Issuers issue Credentials with the consent of
481 the Subjects, or an Entity eligible to act on behalf of the Subject, or when
482 authorized by legislation or regulation.
- 483 3. Participants must be able to assess whether issued Credentials contain accurate
484 reliable and up-to-date information.
- 485 4. Participants must be confident Issuers have adopted and implemented privacy
486 protecting data structures within Credentials to minimize risk of correlation that
487 could result if a Relying Party requests multiple Credentials about a Subject,
488 whether issued by one or more Credential Issuer.

- 489 5. Participants must be confident that compromised or invalid Credentials are
490 addressed in an appropriate and timely manner, and that Credentials are only
491 rendered unusable under legitimate circumstances.
- 492 6. Participants must be confident that information they share with other Participants,
493 or that is stored in Repositories or Verifiable Registries, is not used by a Service
494 Provider or Verifier except as directed by the express consent of the Subject, or
495 an entity authorized to act on their behalf, or when authorized by legislation or
496 regulation. For example, Participants must not use Credentials with which they
497 have been entrusted to impersonate the Subjects, or collude with other
498 Participants to aggregate or share information without such consent.

499 **4. Trusted Processes**

500 The PCTF promotes trust through a set of auditable processes.

501 A process is a business or technical activity, or set of activities, that transforms an input
502 condition to an output condition upon which other processes often depend. A condition
503 is a particular state or circumstance relevant to a Trusted Process. A condition may be
504 an input, output, or dependency relative to a Trusted Process. Conformance Criteria
505 specify what is required to transform an input condition into an output condition.
506 Conformance Criteria specify, for example, what is required for the Register Digital
507 Identity Wallet process to transform a Verifiable Digital Identity Wallet input condition to
508 a Digital Identity Wallet output condition.

509 A process is designated a Trusted Process when it is assessed and certified as
510 conforming to Conformance Criteria defined in a PCTF conformance profile. The
511 integrity of a Trusted Process is paramount because many participants may rely on the
512 output of the process, often across jurisdictional, organizational, and sectoral
513 boundaries, and over the short-term and long-term.

514 The PCTF Digital Wallet component defines the following trusted processes in 3 broad
515 categories:

516 **Wallet Instantiation and Security Processes**

- 517 1. Create Digital Wallet
518 2. Register Digital Wallet
519 3. Authentication

520 **Credential Management and Use Processes**

- 521 1. Request Verifiable Credential
522 2. Store Verifiable Credential
523 3. Manage Verifiable Credential
524 4. Display Verifiable Credential

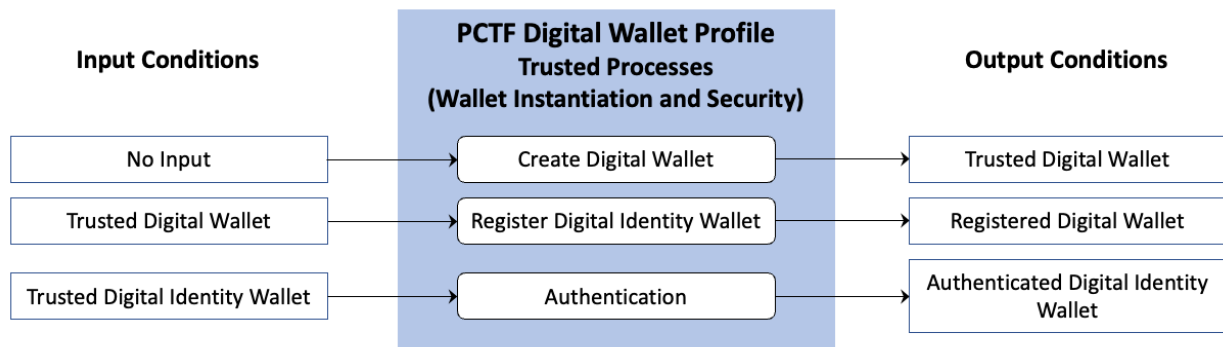
- 525 5. Render Verifiable Credential
- 526 6. Present Proof

527 **Consent Management Processes**

- 528 1. Included in the Present Proof process.

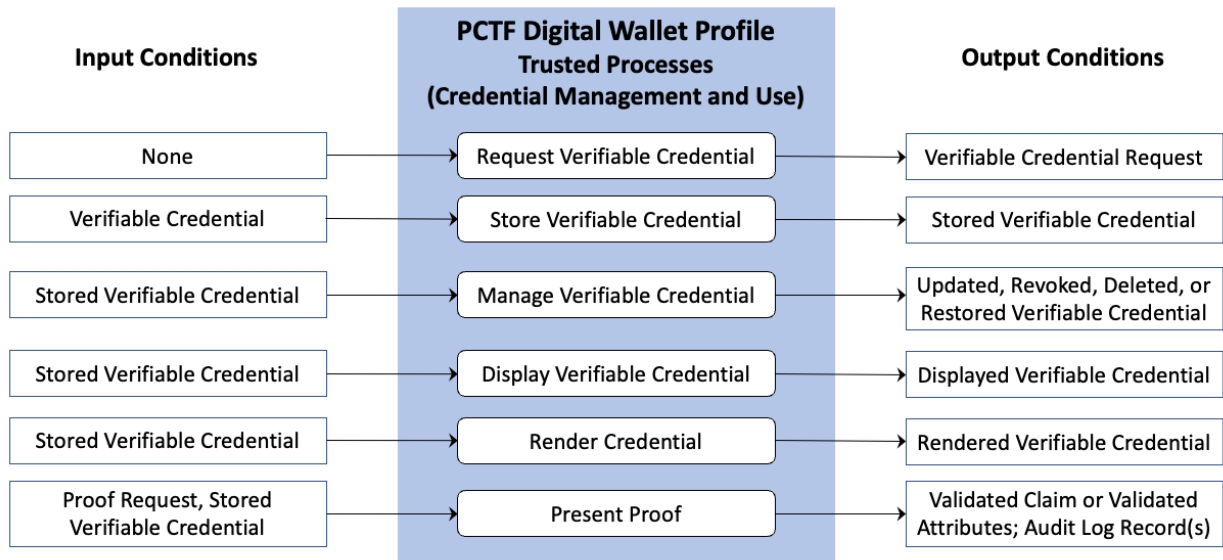
529 **4.1 Conceptual Overview**

530 Figures 3 and 4 provide a conceptual overview, and the logical organization of, the
531 PCTF Digital Wallet Trusted Processes.



532

533 **Figure 3: Digital Wallet Instantiation and Security Trusted Processes**



534

535 **Figure 4: Digital Wallet Credential Management and Use Trusted Processes**

536 **4.2 Process Descriptions**

Status: Draft Recommendation

537 The following sections define the PCTF Digital Identity Wallet Component's Trusted
538 Processes. The PCTF Digital Identity Wallet Conformance Profile specifies the
539 Conformance Criteria against which these processes can be assessed.

540 Trusted Processes are defined using the following structure:

- 541 1. **Description:** A descriptive overview of the process
- 542 2. **Inputs:** Data that is consumed and/or acted upon on by the process
- 543 3. **Outputs:** Data that is created by the process
- 544 4. **Dependencies:** Other processes which must execute prior to the process
545 described in the section, normally because they produce one or more required
546 Inputs

547 **4.2.1 Wallet Instantiation and Security Processes**

548 **Create Digital Wallet**

549 Digital Identity Wallet Creation is the process of creating a wallet that can be verified by
550 a Verifier. Creation may involve installation of software on a mobile or non-mobile
551 device or generating an instance of a wallet on a server.

Inputs	None
Outputs	Trusted Digital Wallet
Dependencies	No Dependencies

552 **Register Digital Identity Wallet**

553 Digital Identity Wallet Registration is the process of a Holder registering a wallet with an
554 Issuer, Verifier or Verifiable Data Registry. Once this process is complete, the Holder
555 will have a Registered Digital Wallet which can be persistently managed by the
556 Registration Service of the Issuer, Verifier or Verifiable Data Registry.

Inputs	Trusted Digital Wallet
Outputs	Registered Digital Wallet
Dependencies	Create Digital Wallet

557 **Authentication**

558 This process establishes an authentication control that enables an Owner to bind
559 Credentials to a Digital Identity Wallet. This binding ensures that the Owner is in control
560 of the Digital Identity Wallet and is authorized to possess, control, and Present the
561 Credentials being bound to that wallet.

562 The output of this process must be cryptographically verifiable.

Inputs	Trusted Digital Identity Wallet
Outputs	Authenticated Digital Identity Wallet
Dependencies	

563 **4.2.2 Credential Management and Use Processes**

564 **Request Verifiable Credential**

565 Through this process a Wallet Holder requests a Credential from an Issuer. The
566 assurance of the request may be enhanced by verifying the attributes of the Digital
567 Identity Wallet, a Verified Person Record and the record of binding as a prerequisite to
568 the Credential request.

Inputs	
Outputs	Verifiable Credential Request
Dependencies	Create Digital Wallet

569 **Store Verifiable Credential**

570 Through this process a Verifiable Credential is secured and stored by a Digital Identity
571 Wallet. In cases where High levels of assurance are required processes and
572 technologies can be implemented as a prerequisite to securing the credential.

Inputs	Verifiable Credential
Outputs	Stored Verifiable Credential
Dependencies	Create Digital Wallet, Request Verifiable Credential

573 **Manage Verifiable Credential**

574 The PCTF recognized the dynamic nature of Credentials which may be stored in a
575 Digital Wallet. The Manage Verifiable Credential process ensures that Credentials and
576 Attributes stored in Digital Wallets contain accurate and timely information. Through the
577 Manage Verifiable Credential process a Verifiable Credential that is secured and
578 accessed by a Digital Identity Wallet can be:

- 579 1. Updated: Bringing a Verifiable Credential's attributes to date via the Credential's
580 Issuer

- 581 2. Revoked: The procedure triggered by an issuer to revoke a Verifiable credential
- 582 and notify the Verifiable Credential Holder
- 583 3. Expired: The procedure triggered by an Issuer for Notice, and expiration of, an
- 584 expired Credential
- 585 4. Restored: The procedure used by an Issuer or Digital Identity Wallet Holder to
- 586 restore a Verifiable Credential
- 587 5. Deleted: The procedure used by a Digital Identity Wallet Holder for deleting a
- 588 Verifiable Credential

589 These functions should only be available to the legitimate Holder of the Credentials (i.e.,
590 the Owner bound to the Digital Identity Wallet).

Inputs	Stored Verifiable Credential
Outputs	Updated, Revoked, Deleted, or Restored Verifiable Credential
Dependencies	Store Verifiable Credential

591 **Display Verifiable Credential**

592 This process retrieves a Credential from a Digital Wallet and displays it for the Owner.

Inputs	Stored Verifiable Credential
Outputs	Displayed Verifiable Credential
Dependencies	Store Verifiable Credential, Render Verifiable Credential

593 **Render Verifiable Credential**

594 This process establishes a particular state or condition for a secured Credential and
595 displays it in a format that can be read and understood by a human.

Inputs	Stored Verifiable Credential
Outputs	Rendered Verifiable Credential
Dependencies	Store Verifiable Credential

596 **Present Proof**

597 A Digital Wallet must be able to present proof of Holder (i.e.; the Wallet’s Owner) Claims
598 (signed credentials) to a Verifier in a compatible format to satisfy a verifier proof
599 request. Key compatibility considerations include format of the Credentials, signature
600 scheme, acceptable issuer for each requested claim and if Selective Disclosure is
601 supported or not. Ideally the Wallet (and Issuer) will support a two-way negotiation

602 process that satisfies both the wallet and Verifier policies as opposed to a fixed one-
603 time exchange.

604 A Proof is a tamper evident presentation of the requested claims that the Verifier can
605 validate via the appropriate cryptographic process. If selective disclosure is supported,
606 then only the specific claims requested by the Verifier can be shared. Otherwise, the full
607 set of credentials required to satisfy the proof request must be shared. The latter
608 presents the risk of sharing personal information for which the verifier has no business
609 need.

610 Prior to accepting a proof request the Holder must consent to sending the requested
611 information to the Verifier. An audit log, accessible by the Holder, must record the time
612 of the transaction, claims requested and presented, verifier details, success status and
613 receipt if provided. Optionally the audit log may persist and present a method to review
614 and revoke consent.

Inputs	Proof Request, Stored Verifiable Credential
Outputs	Verifiable Presentation
Dependencies	Store Verifiable Credential, Express Consent

615 **4.2.3 Consent Processes**

616 The PCTF Notice and Consent component is the authoritative source for Notice and
617 Consent conformance criteria. Notice and Consent conformance criteria will not be
618 provided as part of the Digital Wallet Conformance Criteria unless they are unique to
619 interaction with Digital Wallets. Requesting consent to present a credential proof to a
620 verifier is included in the Present Proof process.

621 **5. References**

622 This section lists all external standards, guidelines, and other documents referenced in
623 this PCTF component.

624 **Note**

- 625 • Where applicable, only the version or release number specified herein applies to
626 this PCTF component.

627 This component of the PCTF leverages the skills, experience, and lessons learned of
628 other organizations working to improve this domain and has taken into consideration
629 material from the following sources:

- 630 • CIO Strategy Council: [CAN/CIOSC 103-1:2020 Digital Trust And Identity – Part](#)
- 631 [1: Fundamentals](#)
- 632 • Government of Canada, Treasury Board of Canada Secretariat: [Public Sector](#)
- 633 [Profile of the Pan-Canadian Trust Framework Version 1.1](#)
- 634 • W3C: [Verifiable Credentials Data Model 1.0](#)
- 635 • W3C: [Decentralized Identifiers \(DIDs\)](#)

636 6. 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
0.03	03-10-2022	PCTF Digital Wallet Design Team	Removed duplication of LOA from the Overview, see the Conformance Profile
1.0	03-30-2022	PCTF Digital Wallet Design Team	TFEC approves as Draft Recommendation V1.0

637