



PCTF Trust Registries 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 **Table of Contents**

27 **1. Introduction 3**

28 **2. Purpose, Context and Scope 3**

29 **2.1 Purpose.....3**

30 **2.2 Context.....3**

31 **2.3 Scope4**

32 2.3.1 In-Scope Topics 4

33 2.3.2 Out-of-Scope Topics 5

34 **3. Relationship to the Pan-Canadian Trust Framework 5**

35 **4. Conventions 6**

36 **4.1 Abbreviations 6**

37 **4.2 Terms and Definitions 7**

38 **5. References 8**

39 **6. Revision History 9**

40

41

42

43

44

45

46

47

48 1. Introduction

49 This document provides an overview of the PCTF Trust Registry Component, a
50 component of the [Pan-Canadian Trust Framework](#) (PCTF). For a general introduction to
51 the PCTF, please see the [PCTF Model Overview](#). The PCTF Model Overview describes
52 the PCTF's goals and objectives and provides a high-level overview of the PCTF.

53 Each PCTF component is described in two documents:

- 54 1. **Overview:** Introduces the subject matter of the component. The overview
55 provides information essential to understanding the Conformance Criteria of the
56 component. This includes definitions of key terms, concepts, and the scope of
57 the component.
- 58 2. **Conformance Profile:** Specifies the Conformance Criteria used to standardize
59 and assess trust elements that are part of this component.

60 This overview provides information related to and necessary for consistent interpretation
61 of the PCTF Trust Registry Conformance Profile.

62 2. Purpose, Context, and Scope

63 2.1 Purpose

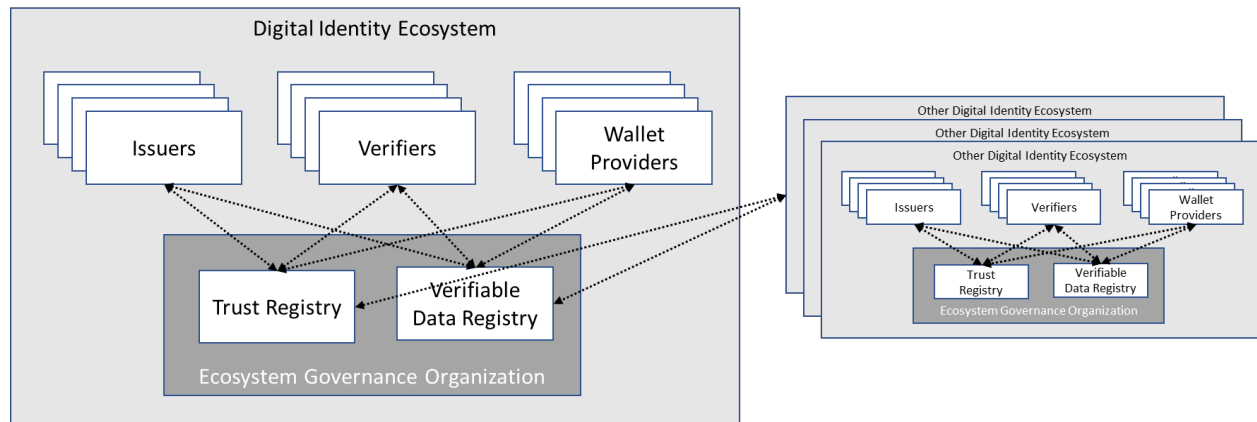
64 The purpose of a Trust Registry is to provide participants of a Digital Identity Ecosystem
65 the means to verify that Ecosystem digital participants are trustworthy. Just as a Verifier
66 needs to know they are dealing with the right person, as outlined in the [Verified Person](#)
67 [component](#) and that their [Credential](#) is valid, the Verifier and the Holder need to know
68 that the organization that is issuing the credential is valid. If an Issuer is listed in a trust
69 registry, this indicates to interested parties (e.g., Verifiers and Holders) that an Issuer
70 can be trusted as an authoritative provider of credentials. Digital Identity Ecosystems
71 and their associated Trust Registries use a Trust Framework (such as the PCTF) to
72 define how Issuers, Verifiers, Holders, and Digital Wallets should or must operate to be
73 considered trustworthy.

74 2.2 Context

75 A Trust Registry is a key component of the new and emerging decentralized digital
76 identity architecture. In this decentralized (or Self Sovereign) architecture a Digital
77 Wallet receives Verifiable Credentials from Issuers and then subsequently provides
78 presentations of these Credentials to Verifiers. In this architecture a Trust Registry
79 provides Issuers, Verifiers, Digital Wallets (and their human Holders), and other Trust
80 Registries the information necessary to verify the identity and status of the other parties

81 as well as the authenticity and status of Credentials and Presentations that a Digital
82 Wallet receives and presents.

83 **Note:** an Issuer, Verifier, or Wallet Provider may be a member of any number of Digital
84 Identity Ecosystems.



85

86

Fig 1: Digital Identity Ecosystems

87 Trust Registries must in turn rely on the legal and foundational sources of digital identity
88 such as Corporate Registries, Drivers Licenses, and Health Card providers. Other
89 components in the PCTF define how these foundational sources of digital identity
90 should or must be used to register digital services within the Trust Registry.

91 **2.3 Scope**

92 **2.3.1 In-Scope Topics**

- 93 • Trust Registry Governance
 - 94 ○ Business Structure – legal framework, business objectives, fees,
 - 95 contracts, and dispute resolution.
 - 96 ○ Ecosystem Scope (Issuers, Verifiers, Wallet Providers, other Trust
 - 97 Registries) – digital service types and industries supported by the
 - 98 Registry.
 - 99 ○ Governance Processes – who operates the governance process and how
 - 100 governance decisions made, communicated, and enforced.
 - 101 ○ Policy and Standards (Trust Framework) – the rules for the digital services
 - 102 supported by the registry and for the registry itself.
- 103 • Trust Registry Operations
 - 104 ○ Technology and Infrastructure Management – how a trustworthy registry’s
 - 105 technical infrastructure should be managed (see [PCTF Infrastructure](#)
 - 106 [\(Technology & Infrastructure\)](#) component).

- 107 ○ Technical Services – the registry technology interfaces that are provided,
108 the registrant schemas, credential schemas, and credential status
109 information that are provided by the registry.
- 110 ● Registration and Certification Management
- 111 ○ Certification/Verification/Trust Mark Services – the process for verifying
112 that the registrant complies with the policies and standards of the
113 Ecosystem.
- 114 ○ Registration – how registrants are identified and authenticated/authorized
115 to use the registry (see PCTF components [Verified Person](#) and [Verified](#)
116 [Organization](#) components).
- 117 ○ 3rd party Trust Registry certification and registration.
- 118 ○ The process for suspending or revoking registration.

119 **2.3.2 Out-of-Scope Topics**

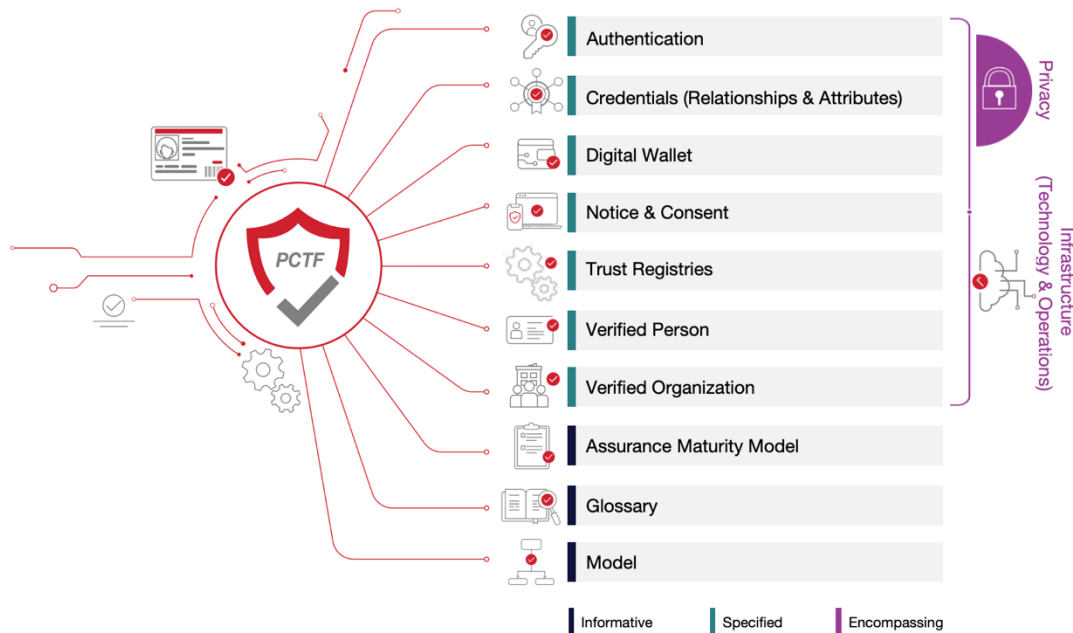
- 120 ● This component does not address requirements of the foundational identity
121 registries that Trust Registries depend upon for identification of entities, such as
122 Corporate Registries, Drivers Licenses, and Birth Registries.
- 123 ● Digital Identity Ecosystems may limit their scope of membership to a particular
124 industry segment. This component does not provide any guidance on how an
125 Ecosystem or Ecosystems might choose or limit their scope of membership.
- 126 ● Digital Identity Ecosystems may have policies regarding whether Verifiers,
127 Issuers, Wallet products, or other Trust Registries will be registered in their trust
128 registry. This component does not provide guidance on whether they should or
129 should not, only that they may be included where required and how they should
130 or must be registered.
- 131 ● Digital Identity Ecosystems may have policies that allow anonymous read access
132 (or not) to the trust registry. This component does not provide guidance on
133 whether they should or should not, only that anonymous access may be allowed
134 where required.

135 **3. Relationship to the Pan-Canadian** 136 **Trust Framework**

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

142 This component references other PCTF components to define the technology,
143 operations, and management processes expected of the Trust Registry. As with other
144 PCTF components, this component does not specify a particular technology stack.

145 Figure 1 is an illustration of the components of the Pan-Canadian Trust Framework.



146

147 **Figure 1. Components of the Pan-Canadian Trust Framework**

148 4. Conventions

149 This section describes and defines key terms and concepts used in the PCTF Trust
150 Registries Component. This information is provided to ensure consistent use and
151 interpretation of terms appearing in this overview, and in the PCTF Trust Registries
152 Conformance Profile.

153 **Notes:**

- 154 • Conventions may vary between PCTF components. Readers are encouraged to
155 review the conventions for each PCTF component they are reading.
- 156 • Key terms and concepts described and defined in this section and the PCTF
157 Glossary are capitalized throughout this document.
- 158 • Hypertext links may be embedded in electronic versions of this document. All
159 links were accessible at time of writing.

160 4.1 Abbreviations

161 The following abbreviations and acronyms appear throughout this overview:

- 162 • **PCTF: Pan-Canadian Trust Framework**

163 **4.2 Terms and Definitions**

- 164 • **Credential**

- 165 ○ A Credential is a set of one or more Claims made about a subject by an
- 166 Issuer. Also known as Verifiable Credentials.

- 167 • **Digital Identity Ecosystem (also referred to as a Network)**

- 168 ○ A formal organization of digital identity participants (Entities) that that
- 169 operate a Trust Registry. As defined in the [PCTF Glossary Final](#)
- 170 [Recommendation V1.0](#), an interconnected system for the exchange and
- 171 verification of digital Identity Information, involving public and private
- 172 sector Organizations that comply with a common Trust Framework for the
- 173 management and use of digital identities, and the Subjects of those digital
- 174 identities.

- 175 • **Digital Wallet**

- 176 ○ A Digital Wallet is a software-based Credential Repository system that
- 177 securely stores information for a Holder. Depending upon the nature of the
- 178 wallet, it may contain information such as Credentials, Verifiable
- 179 Credentials, payment information, and/or passwords. The purpose of a
- 180 Wallet is to securely store Credentials and/or Identity Attributes, and to
- 181 enable the Holder to assemble and prepare Verifiable Presentations.
- 182 Some Wallets might have identity proofing capabilities and/or Agents to
- 183 facilitate the sharing of Credentials they manage.

- 184 • **Digital Wallet Provider**

- 185 ○ An Entity that develops Digital Wallet products for use by Holders. Digital
- 186 Wallet Providers may be Issuers of credentials to Digital Wallets to prove
- 187 their authenticity.

- 188 • **Entity**

- 189 ○ As defined in the [PCTF Glossary Final Recommendation V1.0](#), something
- 190 that has a separate and distinct existence and that can be identified in a
- 191 context.

- 192 • **Holder**

- 193 ○ An Entity that receives Credentials from Issuers, keeps them in their
- 194 possession, and provides Presentations of Credentials to Verifiers.
- 195 Holders use Digital Wallets to receive, keep, and present Credentials.
- 196 Digital Wallets display information from the Trust Registry about Issuers
- 197 and Verifiers to the Holder, so that Holders make informed decisions
- 198 about interacting with Issuers and Verifiers.

- 199 • **Issuer**

- 200 ○ A Registrant that provides Credentials to Holders. Issuers may consider
- 201 information from the Trust Registry about the Holder's Digital Wallet in a
- 202 decision to provide credentials.

- 203 • **Presentation**

- 204 ○ A Presentation is data, typically representing one or more Claims about a
205 Subject, that is derived from one or more Credentials, Verifiable
206 Credentials, Endorsed Relationships, or Verifiable Relationships and
207 shared with a Verifier.
- 208 ● **Registering Party**
- 209 ○ An Entity (usually a real person) that is legally authorized to register an
210 Entity with a Trust Registry.
- 211 ● **Registrant**
- 212 ○ An Entity that is registered in a Trust Registry. Registrants are Issuers,
213 Verifiers, Digital Wallet Providers, and other Trust Registries.
- 214 ● **Trust Registry**
- 215 ○ A digital service operated by a Digital Identity Network that provides
216 information about Registrants. The information can be human readable
217 and/or machine readable such that people and technology services can
218 make informed decisions about the trustworthiness of a Registrant's
219 services (e.g., assurance level as per a Trust Framework). The Trust
220 Registry may include a Verifiable Data Registry component.
- 221 ● **Trust Registry Operations**
- 222 ○ The business and technology processes used to manage the
223 infrastructure and information content of the Trust Registry as well as
224 certify/register Entities in the Trust Registry. The Trust Registry and its
225 operations conform to a Trust Framework such as the PCTF.
- 226 ● **Trust Registry Governance (Governance)**
- 227 ○ The management processes that define the mission, policies, procedures,
228 and standards of an Ecosystem and its Trust Registry.
- 229 ● **Verifiable Data Registry**
- 230 ○ A role a system might perform by mediating the creation and verification of
231 identifiers, keys, and other relevant data, such as verifiable credential
232 schemas, revocation registries, issuer public keys, and so on, which might
233 be required to use verifiable credentials (from W3C).
- 234 ● **Verifier (also referred to as a Relying Party)**
- 235 ○ A Registrant or Entity that receives Presentations of Credentials from
236 Holders and verifies Credentials using information about the Issuers (of
237 the Credentials) from the Trust Registry.

238 5. References

239 This section lists all external standards, frameworks, guidelines, registries, and other
240 documents referenced in this PCTF component. This component of the PCTF leverages
241 the skills, experience, and lessons learned of other organizations working to improve
242 this domain and has taken into consideration material from the following sources:

- 243 ● Trust Over IP (ToIP) [https://github.com/trustoverip/tswg-trust-registry-](https://github.com/trustoverip/tswg-trust-registry-tf/blob/main/docs/ToIP%20Trust%20Registry%20V1%20Specification.md)
244 [tf/blob/main/docs/ToIP%20Trust%20Registry%20V1%20Specification.md](https://github.com/trustoverip/tswg-trust-registry-tf/blob/main/docs/ToIP%20Trust%20Registry%20V1%20Specification.md)

- 245 • Decentralized Identity Foundation (DIF) Credentials Working Group
246 • <https://trustoverip.github.io/essiflab/glossary> (<https://essif-lab.eu>)

247 **Note:** where applicable, only the version or release number specified herein applies to
248 this PCTF component.

249 6. Revision History

Version	Date	Author(s)	Comment
0.01	2022-07-19	PCTF Trust Registries Design Team	Initial Discussion Draft created by the PCTF Trust Registries Design Team
0.02	2022-08-22	PCTF Trust Registries Design Team	Updated version to incorporate Design Team feedback
1.0	2023-03-01	PCTF Trust Registries Design Team	TFEC approves as Draft Recommendation V1.0

250