PCTF Trust Registries Component Overview

Document Status: Final Recommendation V1.0

In accordance with the DIACC Operating Procedures, Final Recommendations are a deliverable that represents the findings of a DIACC Expert Committee that have been approved by an Expert Committee and have been ratified by a DIACC Sustaining Member Ballot.

This document has been developed by DIACC's Trust Framework Expert Committee (TFEC). The TFEC operates under the controlling policies of the DIACC. 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 DIACC.ca.

Table of Contents

1. Introduction

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

Each PCTF component is described in two documents:

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

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

2. Purpose, Context, and Scope

2.1 Purpose

The purpose of a Trust Registry is to provide participants of a Digital Identity Ecosystem the means to verify that other Ecosystem participants are trustworthy. Participants registered in the Trust Registry include Issuers, Verifiers, Wallet Providers, and other Trust Registries. As an example, if an Issuer is listed in a Trust Registry, this indicates to interested parties (e.g., Verifiers and Holders) that an Issuer can be trusted (to a defined degree) as a recognized provider of Credentials. If a Verifier is listed in a Trust Registry this indicates to Holders that the Verifier can be trusted to receive Credential proofs. If a Wallet Provider is listed in a Trust Registry (perhaps as an Issuer of wallet credentials) then this indicates to participants (Issuers, Verifiers, and Holders) that the Digital Wallet product is trustworthy. Digital Identity Ecosystems and their associated Trust Registries use a Trust Framework (such as the PCTF) to define how Issuers, Verifiers, Holders, and Digital Wallets should or must operate to be considered trustworthy.

Note: a Digital Identity Ecosystem may operate a Verifiable Data Registry or equivalent technology that provides machine readable information about Ecosystem credentials to enable processing of Verifiable Credentials and Verifiable Presentations. Requirements for a Verifiable Data Registry or equivalent technology are not in scope for this component.

2.2 Context

A Trust Registry is a key component of the new and emerging decentralized digital identity architecture. In this decentralized (or Self Sovereign) architecture, a Holder receives Verifiable Credentials from Issuers and then subsequently provides presentations of these Credentials to Verifiers. In this architecture, a Trust Registry provides Issuers, Verifiers, Holders, and other Trust Registries the information necessary to verify the identity and status of the other parties in the Ecosystem.

Note: an Issuer, Verifier, or Holder may be a member of any number of Digital Identity Ecosystems. The conceptual diagram below shows the parties a Trust Registry interacts with, but is not meant to show data transfers of a specific technical implementation. Also, Ecosystem participants can take on one or more Issuer, Verifier, and Holder roles.

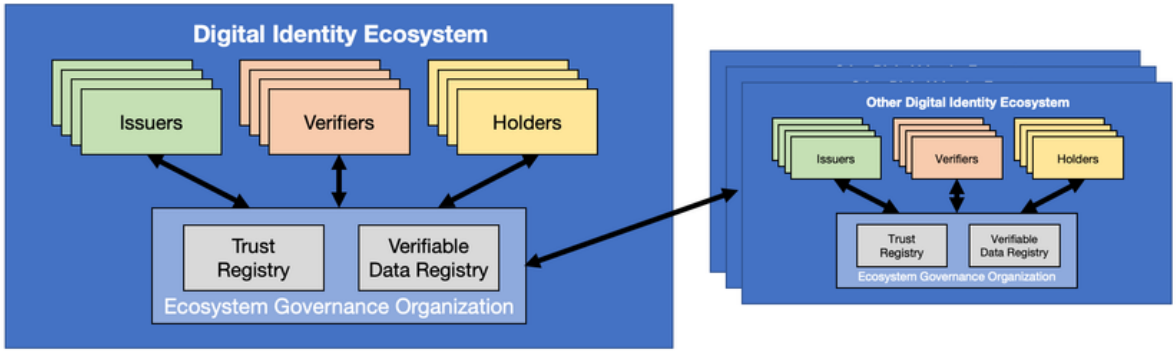

Figure 1. Digital Identity Ecosystems

Trust Registries must in turn rely on recognized sources of digital identity such as professional bodies, corporate registries, drivers licenses, and health card providers. Other components in the PCTF define how these sources of digital identity should or must be used to register participants within the Trust Registry (see section 3 below).

2.2.1 Example Ecosystems and Participants

The following Digital Identity Ecosystem examples are listed to provide additional context for the reader.

- Post-secondary academic Institutions may establish a governance organization to operate a Trust Registry. Post-secondary academic Institutions across Canada may establish a governance organization to operate a Trust Registry. The Trust Registry could have academic institutions as Issuers of student and faculty role and academic Credentials (e.g., transcripts and degrees). Entities needing to validate a role or academic credential issued by a Canadian post-secondary institution, would be able to check this trust registry to confirm the issuer of the

credential was valid. In this ecosystem students, student applicants, faculty, and employees of academic institutions would be Holders of Credentials.
- Health care sectors may a establish governance organization to operate a Trust Registry. The Trust Registry could have professional bodies (e.g., Medical Council of Canada) as Issuers of professional Credentials for health care providers and hospitals, laboratories, pharmacies, and private health care organizations as Verifiers. In this ecosystem, patients, health care providers, and employees of health care services would be Holders of Credentials.
- Professional associations, such as the Law Society of a Province, may establish a Trust Registry to enable their members to securely access services hosted by registered Verifiers related to their profession.

Note: in these examples we would expect that these Ecosystems would in turn would depend on other Ecosystems (and their Trust Registries) that include personal and business credentials issued by government identity Issuers.

2.2.2 Need for Interoperability

As a key requirement in the decentralized identity architecture, with its interconnection with many Holders, Digital Wallets, Issuers, Verifiers, and other trust registries, Ecosystems must strive for interoperability (locally, regionally, and internationally). Adherence to recognized industry standards must be an important goal for Ecosystem governance organizations and this is reflected in many of the compliance criteria for Trust Registries. In addition, staying alive to emerging technology developments will be an important activity for Ecosystem governance organizations to prepare for future interoperability.

2.3 Scope

2.3.1 In-Scope Topics

- Trust Registry Governance
    - Business Structure – legal framework, business objectives, fees, contracts, and dispute resolution.
    - Ecosystem Scope (Issuers, Verifiers, Wallet Providers, other Trust Registries) – digital service types and industries supported by the Registry.
    - Governance Processes – who operates the governance process and how governance decisions are made, communicated, and enforced.
    - Policy and Standards – the rules for the digital services supported by the Registry and for the Registry itself, including authorization to issue credentials.
- Trust Registry Operations

    - Technology and Infrastructure Management – how a trustworthy Registry's technical infrastructure should be managed (see PCTF Infrastructure (Technology & Infrastructure) component).
    - Technical Services – the Registry technology interfaces that are provided, the registrant schemas, credential schemas, interoperability capability, and credential status information that are provided by the Registry.
- Registration and Certification Management
    - Certification/Verification/Trust Mark Services – the process for verifying that the registrant complies with the policies and standards of the Ecosystem.
    - Registration – how registrants are identified and authenticated/authorized to use the Registry (see PCTF Verified Person and Verified Organization components).
    - Certification and registration of other Trust Registries.
    - The process for suspending or revoking registration.

2.3.2 Out-of-Scope Topics

- This component does not address requirements of the identity registries that Trust Registries depend upon for identification of entities, such as Corporate Registries, Drivers Licenses, and Birth Registries.
- Digital Identity Ecosystems may
    - limit their scope of membership to a particular industry segment. This component does not provide any guidance on how an Ecosystem or Ecosystems might choose or limit their scope of membership.
    - have policies regarding whether Verifiers, Issuers, Wallet products, or other Trust Registries will be registered in their Trust Registry. This component does not provide guidance on whether they should or should not, only that they may be included where required and how they should or must be registered.
    - have polices governing what credentials registered issuers are authorized to provide. This component does not provide guidance on whether they should or not, only that these policies may be included where required, including how this authority would be verified.
    - have policies that allow anonymous read access (or not) to the Trust Registry. This component does not provide guidance on whether they should or should not, only that anonymous access may be allowed where required.
- Requirements for Verifiable Data Registries and equivalent technologies are not in scope.

3. Relationship to the Pan-Canadian Trust Framework

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

This component references other PCTF components to define the technology, operations, and management processes expected of the Trust Registry as follows:

- The PCTF Authentication component defines how the Trust Registry should/must authenticate users of the Trust Registry digital services.
- The PCTF Notice and Consent component defines how the Trust Registry should provide notice and consent regarding information management.
- The PCTF Digital Wallet component defines how the Digital Wallet product should/must use a Trust Registry.
- The PCTF Verified Person component defines how the Trust Registry should identify registering parties and other users of the Trust Registry digital services.
- The PCTF Verified Organization component defines how the Trust Registry should identify organizations (and authorized registering parties) that are being registered.

As with other PCTF components, this component does not specify a particular technology stack.

Figure 1 is an illustration of the components of the PCTF.

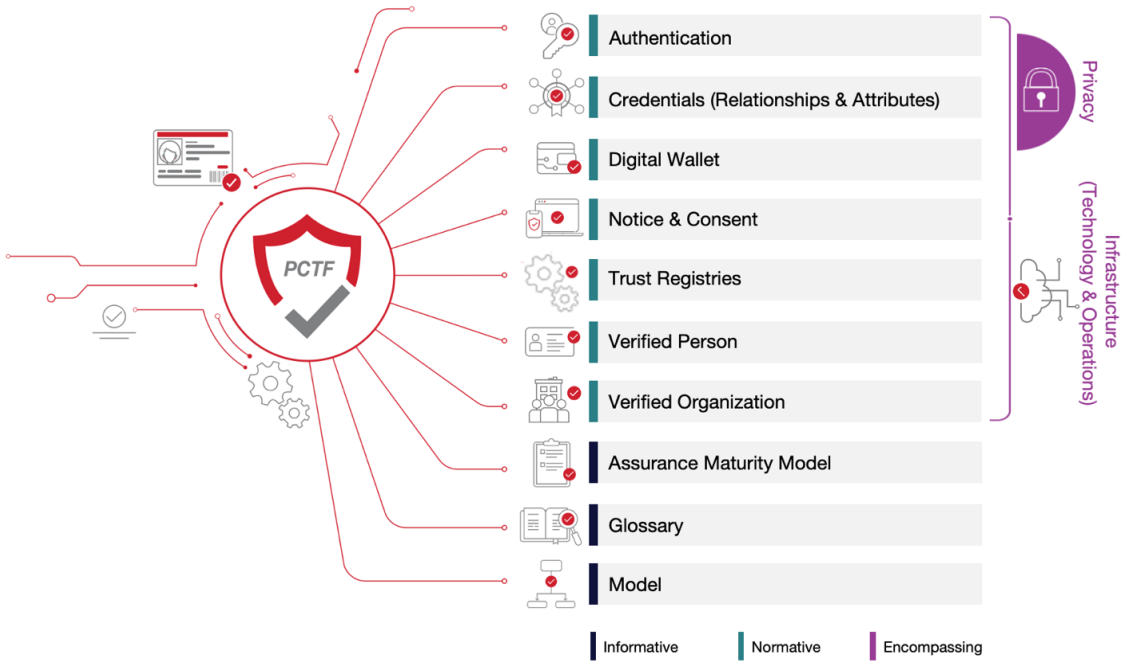

Figure 1. Components of the Pan-Canadian Trust Framework

4. Conventions

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

Notes:

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

4.1 Abbreviations

The following abbreviations and acronyms appear throughout this overview:

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

4.2 Terms and Definitions

Credential

- A Credential is a set of one or more claims made about a subject by an Issuer. Also known as verifiable Credentials. The authorship of a verifiable Credential can be cryptographically verified. Verifiable Credential presentations can also be cryptographically verified.

Digital Identity Ecosystem (also referred to as a Network)

- A formal organization of digital identity participants (Entities) that operate a Trust Registry. As defined in the PCTF Glossary Final Recommendation V1.0, an interconnected system for the exchange and verification of digital Identity Information, involving public and private sector organizations that comply with a common Trust Framework for the management and use of digital identities, and the Subjects of those digital identities.

Digital Wallet

- A Digital Wallet is a software-based Credential repository system that securely stores information for a Holder. Depending upon the nature of the wallet, it may contain information such as Credentials, verifiable Credentials, payment information, and/or passwords. The purpose of a Digital Wallet is to securely store Credentials and/or identity attributes, and to enable the Holder to assemble and present Verifiable Presentations to Verifiers. Some Wallets might have identity proofing capabilities and/or Agents to facilitate the sharing of Credentials they manage. For Digital Wallet requirements see the Digital Wallet Conformance Criteria.

Digital Wallet Provider

- An Entity that develops Digital Wallet products for use by Holders. Digital Wallet Providers may be Issuers of Credentials to Digital Wallets to prove the authenticity of the wallet product to Issuers and Verifiers.

Entity

- As defined in the PCTF Glossary Final Recommendation V1.0, something that has a separate and distinct existence and that can be identified in a context. In this context an Entity is a Digital Identity Ecosystem, Issuer, Holder, or Verifier (and an Entity may perform more than one of these roles in the Ecosystem).

Holder

- An Entity that receives Credentials from Issuers, keeps them in their possession, and provides presentations of Credentials to Verifiers. Holders use Digital Wallets to receive, keep, and present Credentials. Digital Wallets display information from the Trust Registry about Issuers and Verifiers (such as their legal identity, assurance capability, and their information management policies), so that Holders can make informed decisions about the safety of interacting with Issuers and Verifiers.

Issuer

- A Registrant that can assert claims about Holders, can create Credentials from those claims, and can send these Credentials to Holders.

Registering Party

- An Entity (usually a real person) that is authorized to register an Entity with a Trust Registry (such as director of a company or an employee who has been delegated with this authority).

Registrant

- An Entity that is registered in a Trust Registry. Registrants are Issuers, Verifiers, Digital Wallet Providers, and other Trust Registries.

Trust Registry

- A digital service operated by a Digital Identity Ecosystem that provides information about Registrants. The information can be human readable and/or machine readable such that people and organizations (operating technology services) can make informed decisions about the trustworthiness of a Registrant's services (e.g., assurance level, transparency, and audit status as per a Trust Framework). For example, Holders can make informed decisions prior to interacting with Issuers and Verifiers and Verifiers can make informed decisions about accepting verifiable Credential presentations from Holders (and the Issuers of the Credential).

Trust Registry Operations

- The business and technology processes used to manage the infrastructure and information content of the Trust Registry as well as certify/register Entities in the Trust Registry. The Trust Registry and its operations conform to a Trust Framework such as the PCTF.

Trust Registry Governance (Ecosystem Governance)

- The management processes that define the mission, policies, procedures, and standards of an Ecosystem and its Trust Registry.

Verifiable Data Registry

- A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on, which might be required to use verifiable Credentials (from W3C).

Verifiable Presentation

- A Verifiable Presentation is data, typically representing one or more claims about a Subject, that is derived from one or more Verifiable Credentials, and is provided by Holders to Verifiers.

Verifier (also referred to as a Relying Party)

- A Registrant or Entity that requests Verifiable Presentations from Holders, receives Verifiable Presentations from Holders, and verifies Verifiable Presentations. Verifiers use information about the Issuers of the associated

verifiable Credentials from a Trust Registry and/or Verifiable Data Registry to perform the verification of Verifiable Presentations.

5. References

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

- Trust Over IP (ToIP) https://trustoverip.org/ e
- Decentralized Identity Foundation (DIF) Credentials Working Group
- https://trustoverip.github.io/essiflab/glossary (https://essif-lab.eu)
- World Wide Web Consortium (W3C)
- ISO/IEC 20000-1:2018 Standard

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

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
1.1	2023-05-23	PCTF Trust Registries Design Team	Updated version to incorporate feedback received from the public Call for Comments and IPR Review period
1.0	2023-08-30	PCTF Trust Registries Design Team	TFEC approves as Candidate for Final Recommendation V1.0

1.0	2023-11-10	PCTF Trust Registries Design Team	Approved as Final Recommendation V1.0 through DIACC Sustaining Member Ballot