



PCTF Trust Registries

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 was developed by DIACC's [Trust Framework Expert Committee](#) with input from the public gathered and processed through an open peer review process. 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](#) | © 2023

Table of Contents

- 1. Introduction..... 3**
- 2. Purpose, Context, and Scope 3**
 - 2.1 Purpose..... 3**
 - 2.2 Context..... 3**
 - 2.2.1 Example Ecosystems and Participants.....4
 - 2.2.2 Need for Interoperability.....5
 - 2.3 Scope 5**
 - 2.3.1 In-Scope Topics5
 - 2.3.2 Out-of-Scope Topics6
- 3. Relationship to the Pan-Canadian Trust Framework 6**
- 4. Conventions 8**
 - 4.1 Abbreviations 8**
 - 4.2 Terms and Definitions 8**
- 5. Introduction to the PCTF Trust Registries Conformance Profile..... 11**
 - 5.1 Conformance Criteria Keywords 11**
- 6. Levels of Assurance 12**
- 7. Conformance Criteria..... 12**
- 8. References 20**
- 9. Revision History 20**

1. Introduction

Content herein concerns itself with the domain specific topic for this Pan-Canadian Trust Framework (PCTF) component. The overview section provides information related to and necessary for consistent interpretation of the included conformance criteria. For a general introduction to the PCTF, please see the PCTF Overview that describes the background, purpose, scope, principles, and objectives of the framework.

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.

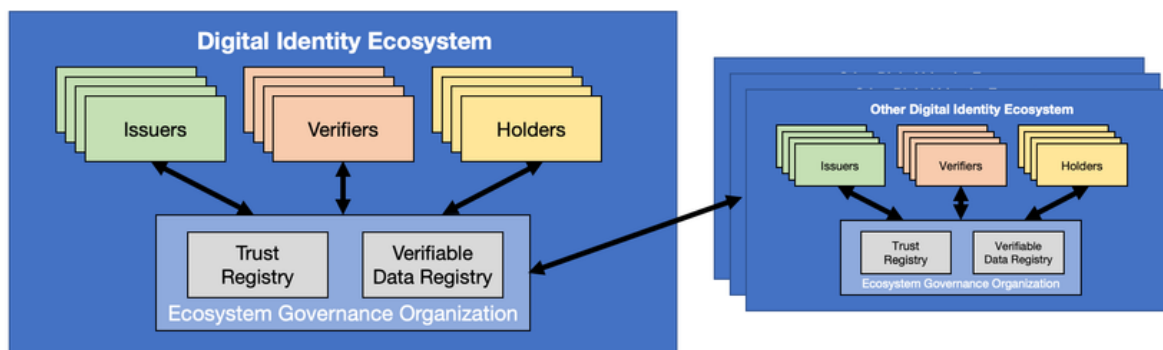


Figure 1. Digital Identity Ecosystems

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 policies 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 2 is an illustration of the components of the PCTF.

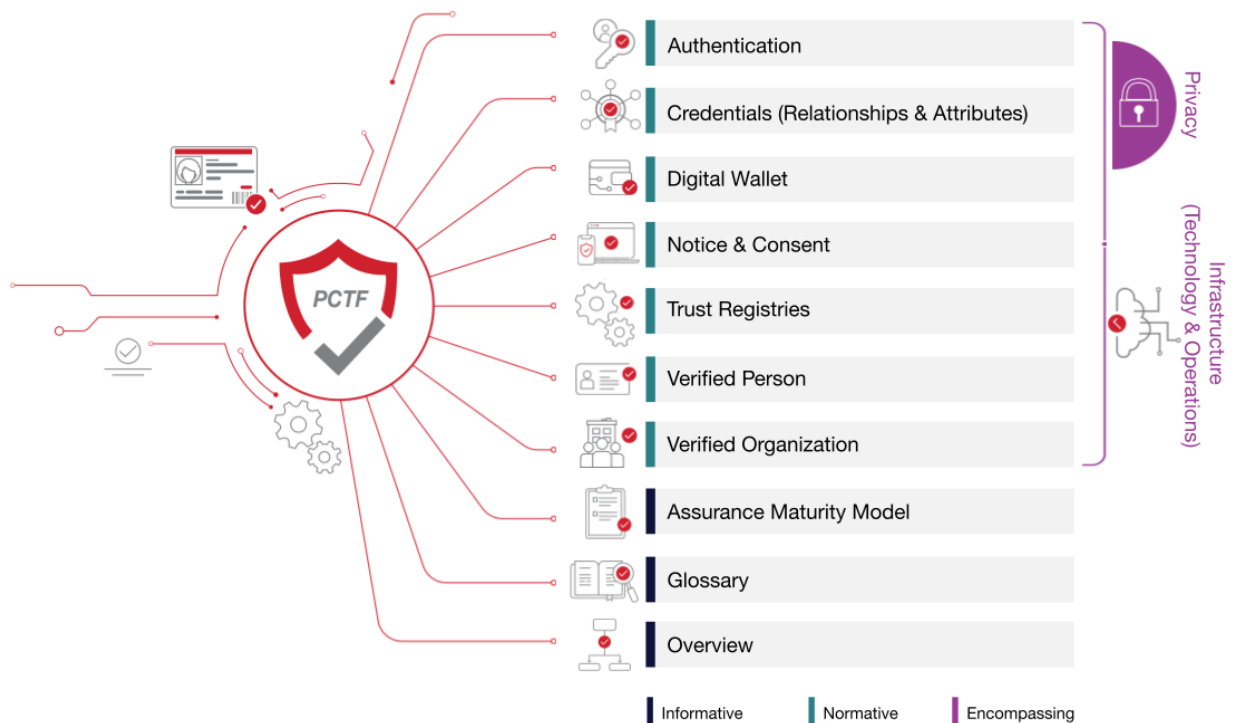


Figure 2. Components of the Pan-Canadian Trust Framework

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. Introduction to the PCTF Trust Registries Conformance Profile

This section specifies the conformance criteria for the Trust Registries component 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 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.

5.1 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.

6. Levels of Assurance

It is essential that Participants in a Digital Identity Ecosystem (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 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 an 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](#).

7. Conformance Criteria

Conformance Criteria are categorized by trust registry functional grouping. For ease of reference, a specific conformance criterion may be referred to by its category and reference number. Example: “BASE1” refers to “Baseline Conformance Criteria reference No. 1”.

Note: Baseline Conformance Criteria are also included as part of this conformance profile.

Reference	Conformance Criteria	Assurance Level			
		LOA1	LOA2	LOA3	LOA4
BASE	These Baseline Criteria Apply to <u>All</u> Trust Registries Processes				
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
GOV	Governance Requirements (Business Structure, Ecosystem Scope, Governance Processes and policies and standards)	LOA1	LOA2	LOA3	LOA4
1	An Ecosystem governance organization (Ecosystem) MUST establish information access policies for the Trust Registry and associated published documents described in this document. This component does not provide guidance on whether an Ecosystem should provide open access or not, just that this policy must be defined and access controls implemented if required.	X	X	X	X
2	An Ecosystem governance organization (Ecosystem) SHOULD be a legally registered business (e.g., Corporation, Partnership, etc.) in the jurisdiction(s) in which it operates, or if the Ecosystem is a public body then there SHOULD be authorizing legislation, and in either case the Ecosystem SHOULD publish this information.	X			
3	An Ecosystem MUST be a legally registered business (e.g., Corporation, Partnership, etc.) in the jurisdiction(s) in which it operates, or if the Ecosystem is a public body, then there MUST be authorizing legislation, and in either case the Ecosystem MUST publish this information.		X	X	X
4	An Ecosystem SHOULD document and publish its beneficial ownership (note: this criteria is not relevant for public bodies).	X			

5	An Ecosystem MUST document and publish its beneficial ownership (note: this criteria is not relevant for public bodies).		X	X	X
6	An Ecosystem SHOULD document and publish its management structure and contact information.	X			
7	An Ecosystem MUST document and publish its management structure and contact information.		X	X	X
8	An Ecosystem SHOULD document and publish its business and policy making processes, committees, and other related processes.	X			
9	An Ecosystem MUST document and publish its business and policy making processes, committees, and other related processes.		X	X	X
10	An Ecosystem MAY document and publish a business plan on an annual basis that is reviewed and approved by the governance body on an annual basis.	X	X	X	X
11	An Ecosystem SHOULD document and publish what types of Entities it will register (Issuers, Verifiers, Wallet Providers, other Trust Registries) and other criteria such as industry, association, or profession.	X			
12	An Ecosystem MUST document and publish what types of Entities it will register (Issuers, Verifiers, Wallet Providers, other Trust Registries) and other criteria such as industry, association, or profession.		X	X	X
13	An Ecosystem SHOULD document and publish the policy and process for verification of the authority of Registrants to issue Credentials or accept Credential presentations.	X			
14	An Ecosystem MUST document and publish the policy and process for verification of the authority of Registrants to issue Credentials or accept Credential presentations.		X	X	X

15	An Ecosystem SHOULD document and make available its financial report and insurance documentation to Registrants. Financial reporting and insurance documentation requirements will vary with the business model of the Ecosystem and the type of Ecosystem organization (e.g., may not be relevant for public bodies).	X	X	X	X
16	An Ecosystem SHOULD document and make available its underwriting policy, if applicable.	X	X	X	X
17	An Ecosystem SHOULD conform to a recognized trust framework such as the PCTF or equivalent.	X			
18	An Ecosystem MUST conform to a recognized trust framework such as the PCTF or equivalent.		X	X	X
19	An Ecosystem SHOULD maintain certification of a recognized trust framework, Trust Mark, or equivalent verification process on an annual basis and publish its status.	X			
20	An Ecosystem MUST maintain certification of a recognized trust framework, Trust Mark, or equivalent verification process on an annual basis and publish its status.		X	X	X
21	An Ecosystem SHOULD document and publish service descriptions and service levels for all business processes and technology services.	X			
22	An Ecosystem MUST document and publish service descriptions and service levels for all business processes and technology services.		X	X	X
23	An Ecosystem SHOULD document and publish a statement of how it does not unjustly discriminate against any party and how it maintains its impartiality in its business processes.	X	X	X	X

24	An Ecosystem SHOULD operate a risk management program, maintain a risk registry, and have an annual review and approval by the governing body.	X			
25	An Ecosystem MUST operate a risk management program, maintain a risk registry, and have an annual review and approval by the governing body.		X	X	X
OPS	Trust Registry Operations (Technology and Infrastructure Management and Technical Services)	LOA1	LOA2	LOA3	LOA4
1	A Trust Registry (Registry) SHOULD conform to a recognized industry framework for its technology infrastructure operations such as the PCTF Infrastructure (Technology & Operations) component or the ISO/IEC 20000-1:2018 standard.	X			
2	A Registry MUST conform to a recognized industry framework for its technology infrastructure operations such as the PCTF Infrastructure (Technology & Operations) component or the ISO/IEC 20000-1:2018 standard.		X	X	X
3	A Registry SHOULD maintain an accessible repository (e.g., internet web site) to host all published documents noted in this component.	X	X	X	X
4	A Registry SHOULD demonstrate the authenticity of all documents published, for example using digital signatures.	X	X		
5	A Registry MUST demonstrate the authenticity of all documents published, such as using digital signatures.			X	X
6	A Registry MUST provide human readable versions of published documents described in this component.	X	X	X	X
7	A Registry SHOULD provide machine readable versions of appropriate documents in industry recognized formats and standards.	X	X		

8	A Registry MUST provide machine readable versions of appropriate documents in industry recognized formats and protocols.			X	X
9	A Registry SHOULD provide machine readable information in a manner that prevents tracking and correlation of Holder and Digital Wallet use of Issuers and Verifiers.	X	X	X	X
10	A Registry SHOULD provide information about its identity in a format compliant with recognized industry standards such as the PCTF Verified Organization component.	X			
11	A Registry MUST provide information about its identity in a format compliant with recognized industry standards and frameworks such as the PCTF Verified Organization component.		X	X	X
12	A Registry SHOULD provide Holders, Verifiers, and Issuers with Registry data in recognized industry formats and standards to enable offline transactions between Holders, Issuers, or Verifiers.	X	X		
13	A Registry MUST provide Holders, Verifiers, and Issuers with Registry data in a recognized industry formats and standards to enable offline transactions between Holders, Issuers, or Verifiers.			X	X
14	A Registry SHOULD provide information about Registrants and their status in industry standard formats and protocols.	X			
15	A Registry MUST provide information about Registrants and their status in industry standard formats and standards.		X	X	X
16	An Ecosystem MAY allow Registrants to directly publish information about their digital services in a Registry using industry standard methods and framework assurance processes such as the PCTF Authentication and PCTF Credentials (Relationships & Attributes) components.	X	X	X	X

17	A Registry MAY provide credential status information or links to Credential Status Information.	X	X	X	X
18	A Trust Registry MUST document and publish technical information for Issuers, Verifiers, and Digital Wallet providers to support the development of products that connect to the Registry.	X	X	X	X
19	A Registry SHOULD provide development and test environments for Issuers, Verifiers, and Digital Wallet providers to develop and test their digital products use of the Registry.	X	X	X	X
REG	Registration and Certification Management (Certification/Verification/Trust Mark Services, Registration, Suspension and revocation processes)	LOA1	LOA2	LOA3	LOA4
1	An Ecosystem SHOULD identify Registrants using recognized assurance processes such as the PCTF Verified Organization Component .	X			
2	An Ecosystem MUST identify Registrants using recognized assurance processes such as the PCTF Verified Organization Component .		X	X	X
3	An Ecosystem SHOULD implement processes and controls to ensure Registrant information is current and consistent with legal registrations, legislation, and/or certifications.	X	X		
4	An Ecosystem MUST implement processes and controls to ensure Registrant information is current and consistent with legal registrations, legislation and/or certifications.			X	X
5	An Ecosystem SHOULD identify and authenticate Registering Parties and beneficial owners using framework assurance processes such as the PCTF Verified Person and PCTF Credentials (Relationship & Attributes) components.	X			

6	An Ecosystem MUST identify and authenticate Registering Parties and Beneficial Owners using framework assurance processes such as the PCTF Verified Person and PCTF Credentials (Relationship & Attributes) components.		X	X	X
7	An Ecosystem SHOULD require that Registrants conform to a recognized trust framework such as the PCTF.	X			
8	An Ecosystem MUST require that Registrants conform to a recognized trust framework such as the PCTF.		X	X	X
9	An Ecosystem SHOULD require that Registrants have certification of trust framework conformance using recognized trust certification services such as the Voilà Verified Trustmark Program .	X	X		
10	An Ecosystem MUST require that Registrants have certification of trust framework conformance using recognized trust certification services such as the Voilà Verified Trustmark Program , or use an equivalent certification or verification process.			X	X
11	An Ecosystem SHOULD document and publish registration and certification processes and services available to Registrants, such as the Voilà Verified Trustmark Program .	X	X	X	X
12	An Ecosystem SHOULD verify that Registrants are authorized to issue Credentials or receive Credential presentations according to the Ecosystem policies and include this authorization in the Trust Registry.	X			
13	An Ecosystem MUST verify that Registrants are authorized to issue Credentials or receive Credential presentations according to the Ecosystem policies and publish this in the Registry.		X	X	X

8. 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](https://www.w3.org/))
- [ISO/IEC 20000-1:2018](https://www.iso.org/standard/62453.html) Standard

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

9. 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