PCTF Overview

Document Status: Final V1.0

Table of Contents

1. Introduction

This informative document describes the background, purpose, scope, principles, and objectives of the Digital ID & Authentication Council of Canada (DIACC) Pan-Canadian Trust Framework[1]™ (PCTF).

The PCTF is a set of rules and policies to operate secure, privacy-enhancing, efficient, and trustworthy digital identity assurance, authentication, credential management, and supporting services.

The PCTF has been developed and is maintained through a collaboration of critical stakeholders from the private and public sectors, following standardized and open processes and procedures.

To respond to digital ID and trust related complexities, the PCTF has a modular approach, providing a comprehensive set of documents aligned to the various functionalities and core aspects of identity management services.

2. Background and Purpose

The DIACC is a not-for-profit organization incorporated and registered in Canada[2].

Canadian Finance Minister Flaherty appointed the Task Force for the Payments System Review in 2010, comprised of representatives from the public and private sectors, privacy commissioner's offices, and consumer advocates. One of the key outcomes was the recognition that digital ID and authentication are integral to the success of digital payments and Canada's digital economy.

Following recommendations from the federal government's Task Force for the Payments System Review in 2012, leaders from Canada's public and private sectors decided to form the DIACC to continue the activities of the Electronic Payments Task Force and achieve its vision for a robust, secure, scalable, and privacy-enhancing structure for transacting online.

This non-profit coalition of public and private sector leaders is committed to developing a Canadian digital ID and authentication framework to enable Canada's full and secure participation in the global digital economy.

[1] DIACC, "Trust Framework", *DIACC* [website], 2023, PCTF Documents, <https://diacc.ca/trust-framework/>, accessed September 27, 2023.
[2] DIACC, "Controlling Policies," *DIACC* [website], DIACC By-laws, 2019, <https://diacc.ca/controlling-policies/>, accessed September 27, 2023
[3] Government of Canada, "News", *Canada.ca* [website], 2010, <https://www.canada.ca/en/news/archive/2010/06/minister-finance-announces-task-force-review-payments-system.html>accessed September 27, 2023.

To build trust and enable a robust, secure, interoperable, inclusive, and privacy-enhancing Canadian digital ecosystem, DIACC has created a set of rules, processes, and procedures that describe the specified requirements for service providers in the identity space and define the methodology for performing third-party conformity assessment. These rules are known as the PCTF.

The DIACC collaboratively maintains the PCTF and benefits from the inputs of Canada's federal, provincial, and territorial representatives within the Joint Councils (a multi-jurisdictional collaborative body supported by the Institute for Citizen-Centred Services), the Canadian public sector, international stakeholders, and the broad economic sector.

3. Scope and Applicability

In general, a trust framework enables an ecosystem, community, or marketplace to be interoperable and secure while allowing users to share reliable personal or organizational identity information. Trust frameworks define and standardize processes and practices and specify data protection policies that government agencies, banks, telecommunication companies, health care providers, and businesses agree to follow regarding information assurance practices.

In this context, the PCTF offers a high-level and versatile code of practice that organizations agree to follow to deliver one or more services, which includes best practices, policies, technical specifications, guidance, regulations, and standards. The PCTF enhances digital trust relationships across the Canadian ecosystem based on legal, policy, and technical requirements to which organizations agree to adopt.

The PCTF can be applied to all types of transactions where digital ID or authentication is required, regardless of the target audience, including individuals, citizens, residents, businesses, and government entities.

Parties that have an interest in the PCTF include but are not limited to:

a) Companies or Entities that provide digital ID services, service providers (e.g., identity service providers, identity proofing, credential management services, cloud-based identity and access management, attribute service providers, identity exchanges, wallet providers, federation operators, integration, among others).
b) Customers of the service providers.
c) Government authorities.
d) Audit firms.
e) Relying Parties.
f) Standards Bodies.
g) Consulting firms.
h) National and international stakeholders.
i) Consumers and other members of the public.

Service providers and government entities use the PCTF as part of their risk assessment and implementation of their digital services.

The PCTF requirements for service providers are specified in the conformance criteria volumes owned and published by DIACC. The requirements cover any type of services in the scope of the PCTF Components.

Trust Frameworks establish trust by assessing service providers against their established requirements for their community. To achieve this objective, DIACC offers third-party conformity assessment through its Voilà Verified Certification Program[4] designed around ISO/IEC 17065 based on independent evaluation (third-party audits) to validate the conformity of PCTF criteria and independent review of the audit findings.

4. Structure

The PCTF consists of modular or functional components that can be independently assessed and certified for consideration as trusted components, depending on the service provider's functionality. The PCTF is organized as a suite of informative and normative components[5]. The framework's suite is illustrated in Figure 1. Each normative component includes an overview and conformance criteria.

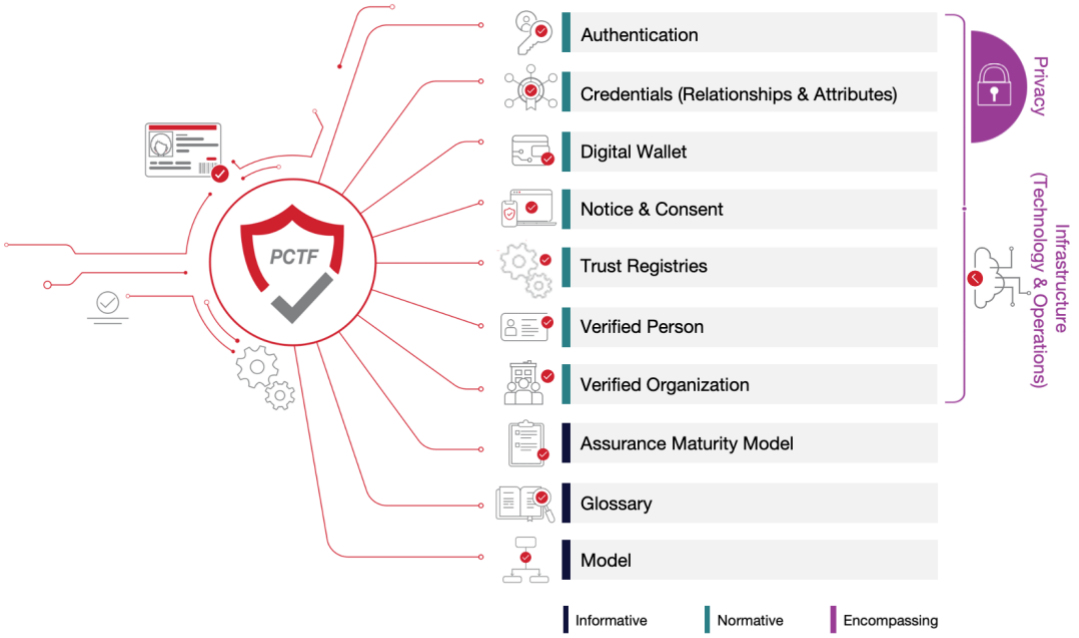

Figure 1. Components of the Pan-Canadian Trust Framework

[4] DIACC, "Certification Program", *DIACC* [website], 2023, <https://diacc.ca/certification-program/>, accessed September 27, 2023.
[5] DIACC, "Trust Framework", *DIACC* [website], 2023, PCTF Documents, <https://diacc.ca/trust-framework/>, accessed September 27, 2023.

5. Objectives

The PCTF addresses Canadian digital ID ecosystem innovation needs and helps to secure the interoperability of public and private sector identity capabilities while prioritizing user-centered design, privacy, security, choice, and convenience of use.

The PCTF facilitates the following outcomes:

- Organizations can reduce risks and costs while offering secure and standardized services, simplifying and ensuring consistency of interactions, transactions, and information sharing between institutions, businesses, and individuals.
- Trustworthiness and interoperability of public and private sector digital trust and identity capabilities.
- Improve user experience and reduce fraud by prioritizing user-centered design, privacy, security, and convenience.
- Widely applicable, outcome-based, technology-agnostic, open, and flexible.
- International alignment with relevant frameworks' policies worldwide to facilitate interoperability and adoption.
- Provide certainty to the market through trusted services that have been subject to DIACC third-party conformity assessment, granting assurance that the services fulfill the specified requirements.
- Protect and promote Canadian values and perspectives in the digital economy. In this context, the PCTF supports the guiding principles[6] that DIACC has identified for a digital ID ecosystem for Canada and solutions within.

6. Development and Maintenance

The PCTF is developed and maintained through an open and multistakeholder collaborative process defined in the DIACC Operating Procedures[7].

The DIACC's Trust Framework Expert Committee (TFEC[8]) is the working group responsible for developing and maintaining the PCTF. The TFEC consists of members from the public and private sectors who work collaboratively through a Peer-Review and Development Process to maintain the PCTF. The TFEC defines the PCTF's informative and normative documents, adhering to DIACC's Operating Procedures, and describes the applicable value propositions across Canada's public and private sectors. The TFEC ensures audibility, suitability, and consistency of its defined conformance criteria operationalized in the DIACC's Certification Program.

[6] DIACC, "Principles", *DIACC* [website],< https://diacc.ca/the-diacc/principles/>, 2015, accessed September 27, 2023.
[7] DIACC, "Controlling Policies," *DIACC* [website], DIACC Operating Procedures, 2020, <https://diacc.ca/controlling-policies/ >, accessed September 27, 2023.
[8] TFEC Charter DIACC TFEC Charter

The PCTF is reviewed by TFEC and DIACC editors regularly as needed, ensuring it is updated with evolving ecosystems, standards, and regulations.

PCTF Conformance Criteria Development Process

The PCTF requirements are developed following an open and standardized process, as specified in Figure 2. These include initial draft development through TFEC Design Teams, TFEC review, DIACC Board approval for public input, revisions to incorporate public feedback, finalize DIACC's Disposition of Comments, and approval from DIACC membership for final publication.

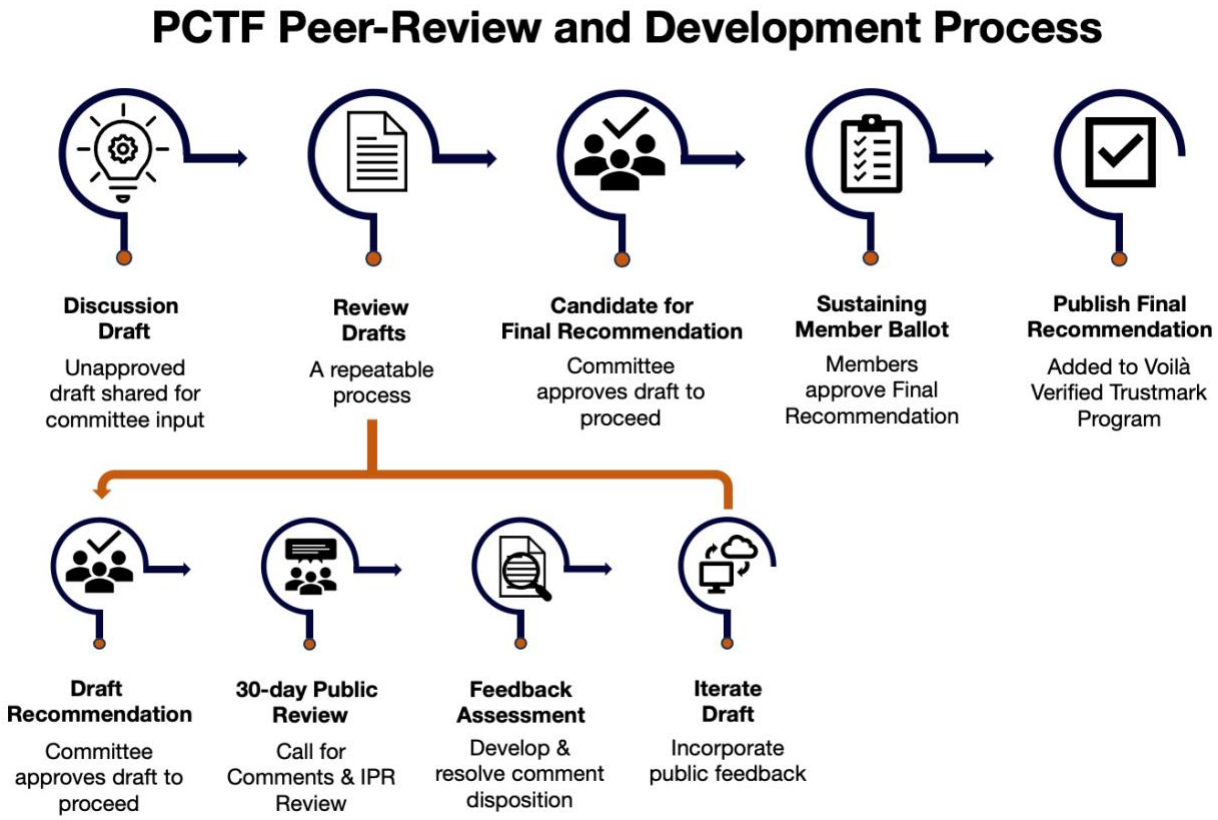

Figure 2. PCTF Peer-Review and Development Process

As specified in the Operating Procedures, reviewing the informative and normative documents is a public and open process where any interested party can participate and provide feedback. The public Call for Comments & IPR Review period is vital to the DIACC multistakeholder model. It provides a mechanism to ensure a balanced representation of interested parties' opinions, views, and suggestions.

In addition to the public comment review periods, DIACC offers an ongoing channel for anyone interested in providing feedback using the PCTF Out of Band Feedback form[9].

[9] PCTF Out of Band Feedback form

This form collects PCTF public community feedback outside the prescribed public review & comment periods. The DIACC team monitors this form's responses every quarter. The DIACC's TFEC will consider comments for inclusion.

7. Considerations

The PCTF conformance criteria must be interpreted "as is". If service providers implement other risk mitigation measures and compensating controls not specified in the PCTF and want to get certified, the comparable or compensating controls must be evaluated. Comparable or compensating controls might be accepted in exceptional cases subject to DIACC auditors' validation and justification.

DIACC is committed to international alignment with the policies and requirements of digital identity frameworks from other jurisdictions and works towards cross-border collaboration to advance interoperability. Depending on the mapping tools developed for identifying the deltas between the different policies and values within the requirements and levels of assurance, DIACC may consider partial recognition of other certifications as input for the audit process to facilitate the adoption and certification of the PCTF.

8. Revision History

Version	Date	Author(s)	Comment
1.0	2023-09-28	PCTF Editor's Office	New document