DIACC CCIAN

PCTF Infrastructure (Technology & Operations) Component Overview

Document Status: Final Recommendation V1.1

In accordance with the DIACC Operating Procedures, a Final Recommendation is 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. 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.

Table of Contents

1. Introduction to the PCTF Infrastructure (Technology & Operations) Component

This document provides an overview of the PCTF Infrastructure (Technology & Operations) Component, a component of the Pan-Canadian Trust Framework (PCTF). For an introduction to the PCTF, please see the PCTF Model. The PCTF Model Overview provides the PCTF's goals and objectives, a high-level model outline of the PCTF, and contextual information.

PCTF components typically consist of two documents:

1. **Component overview** – Introduces the subject matter of the component. It provides informative information essential to understanding the Conformance Criteria of the component. This includes definitions of key terms, concepts, and the trusted processes that are part of the component.
2. **Component conformance profile** – Specifies the Conformance Criteria used to standardize and assess the integrity of the trusted processes that are part of the component.

This overview provides information related to and necessary for consistent interpretation of the PCTF Assessment Component.

1.1 Purpose and Anticipated Benefits

The objective of the PCTF Infrastructure (Technology & Operations) Component is to identify the operational policies, plans, technology and technology operations requirements to support implementation of the principles of the PCTF Profiles in the context of a Digital Identity Ecosystem.

A process that has been certified is a Trusted Process that can be relied on by other participants of the PCTF. The PCTF Conformance Criteria are intended to complement existing privacy legislation and regulations; DIACC-certified participants in the Digital Identity Ecosystem are expected to meet the applicable legislated requirements and regulations in their jurisdictions.

The PCTF Infrastructure (Technology & Operations) Component defines:

- The formal policy and plan artifacts that form the basis of a conforming technology installation and its technology support operations.

- The high-level technology and technology tool capabilities required to support a technology infrastructure delivering service to a Digital Identity Ecosystem.
- The technology support operational tools and characteristics to support an installed technology infrastructure delivering service to a Digital Identity Ecosystem.

1.2 Scope

This section defines the scope of the PCTF Infrastructure (Technology & Operations) Component. In-scope requirements are identified at a high level to illustrate scope, detailed requirements are elaborated in the PCTF Infrastructure (Technology & Operations) Conformance Profile.

1.2.1 In-Scope

This PCTF component will specify conformance criteria that provide general requirements and guidelines regarding the trustworthiness of the IT infrastructure that enables implementation and delivery of the trusted processes defined in other PCTF components. The component's primary subject areas are the security and integrity of technical components. Within these areas of interest, the component's scope includes:

- IT security (as a general consideration).
- Oversight of data collection, validation, storage, and accessibility.
- Audit and logging.
- Prevention of, and response to, IT events that compromise the trustworthiness of the Digital Identity Ecosystem.
- Policies and plans supporting the trustworthy management of technology and technology operations.

1.2.2 Out-of-Scope

The scope of this PCTF component does not include:

- The suitability of specific products to support a given trusted process.
- The suitability of standards, processes, technologies, or technology protocols that may be specific to, or mandated by, an individual Digital Identity Ecosystem.
- Mandating the use of a specific set of standard practices or frameworks to govern technology operations (e.g. IT Infrastructure Library <<ITIL>>, Control Objectives for Information Technology <<COBIT>>).

1.3 Relationship to the PCTF

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 Identity Ecosystem.

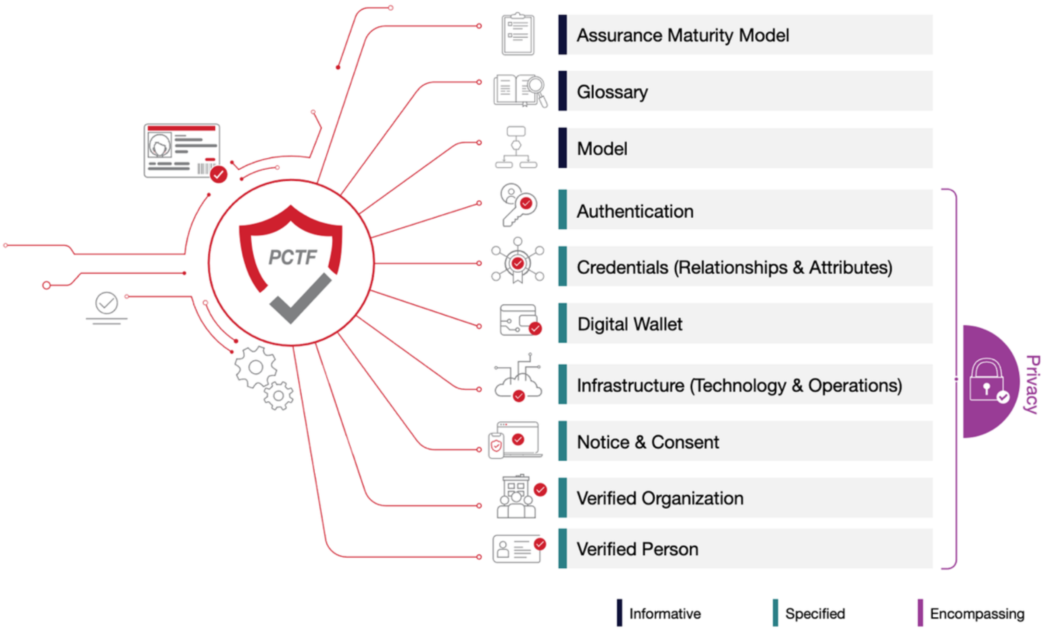

Figure 1 - Components of the Pan-Canadian Trust Framework

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.

2. Infrastructure (Technology & Operations) Conventions

This section describes and defines key terms and concepts used in the PCTF Infrastructure (Technology & Operations) Component. This information is provided to ensure consistent use and interpretation of terms throughout this component.

Note

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

2.1 Terms and Definitions

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

Conformance Criteria

Requirements developed for each of the PCTF Components and used as the basis to assess compliance

Digital Identity Ecosystem

An interconnected ecosystem 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.

Personal Information

Any factual or subjective information, recorded or not, about an identifiable individual (Source: PIPEDA in Brief, Office of the Privacy Commissioner of Canada - What is personal information?).

2.2 Abbreviations

The following abbreviations appear throughout this PCTF component:

- DIACC – Digital ID & Authentication Council of Canada
- COBIT - Control Objectives for Information Technology
- ENISA - European Union Agency for Cybersecurity
- FEDRAMP - Federal Risk and Authorization Management Program
- ITIL - IT Infrastructure Library
- NIST - National Institute of Standards and Technology
- PCTF – Pan-Canadian Trust Framework

3. Conformance Criteria Coverage

Conformance criteria are elaborated in detail in the PCTF Infrastructure (Technology & Operations) Conformance Profile. Requirements were designed to reflect the capabilities and characteristics found in technology operations and governance standards (e.g., ITIL, COBIT) without being so prescriptive that a specific standard is required.

Similarly, public sector standards bodies and their implementation guidance were drawn upon to help define some of the detailed requirements in the Conformance Criteria. These include National Institute of Standards and Technology (NIST) and Federal Risk and Authorization Management Program (FEDRAMP) in the US, European Union Agency for Cybersecurity (ENISA) in Europe, and various Federal Government Directives in Canada. The approach was to derive inspiration from some of the common guidance for technology implementation and management while ensuring that the PCTF Conformance Criteria were generic enough to co-exist in any public or private sector domain.

It is worth noting that the PCTF Infrastructure (Technology & Operations) Conformance Criteria are described in a generic fashion, focusing more on the capabilities required to operate a trusted infrastructure as a platform for delivery of other conforming services within the PCTF. It is expected that organizations wishing to participate in a specific Digital Identity Ecosystem will have additional specific technology and technology operations requirements imposed upon them by the Digital Identity Ecosystem. The identification of a required specific technology product, protocol, or third-party operational standard in an individual Digital Identity Ecosystem is not within the scope of this profile.

The Criteria are organized into three broad categories. These are:

- Policies and Plans - capture the key formal artifacts that elaborate the organization's consistent approach to instantiating and managing the technology and system components that fulfill the role that organization is playing in the Digital Identity Ecosystem.
- Technology – identifies the characteristics and capabilities of required technology components.
- Operations – identifies the characteristics and capabilities required of the operational framework and toolset utilized to play a defined role within a Digital Identity Ecosystem.

3.1 Policy and Plans

The foundation of the technology component of an enterprise architecture is a comprehensive set of organization policies and plans clearly mapped to the business objectives identified in the business components of the enterprise architecture. This profile identifies requirements for formal artifacts and their continuous management in the areas of:

- Risk assessment;
- Audit and accountability;
- Security assessment;
- Disaster or contingency planning;
- Identification and authentication;
- Systems and communication protection;
- Incident response;
- System and information integrity;
- Configuration management;
- Information management;
- System maintenance;
- Technical access control;
- Physical access control; and,
- Personnel security.

At a high level, the most important takeaway from this set of criteria is the need for orderly planning that starts with the identification of objectives in policy statements, supported by formal plans that govern the implementation and operation of technology.

3.2 Technology Criteria

These criteria focus on identifying the generic tools and technology capabilities required to support an operating infrastructure delivering PCTF conforming services. Specific technology products or protocols are not identified as these tend to vary depending on the specific trusted process being delivered in an individual Digital Identity Ecosystem. It is expected that organizations will have additional specific requirements in this area imposed by the Digital Identity Ecosystem in which they wish to operate.

Also, the capabilities that are specific to other PCTF trusted processes (i.e., Authentication, Privacy, Verified Person, etc.) are not elaborated in this Profile. Those criteria are identified in the subject matter-specific PCTF Conformance Profiles. There are several cross-references to other Conformance Profiles where appropriate.

3.3 Technology Operations Criteria

The third category of Conformance Criteria identifies the technology operations and support capabilities required to operate a PCTF conforming infrastructure. Aligned with the policies and plans identified earlier, these capabilities represent the ongoing technology, support and operational characteristics required to deliver on the enterprise capabilities identified in the policies and plans associated with a comprehensive enterprise architecture.

4. References

This Profile was influenced by the standards or standard bodies listed below. Each of the cited organizations includes a document repository containing multiple documents pertaining to the establishment and operation of a technical infrastructure required to support the delivery of service, in this case, to a Digital Identity Ecosystem.

Note:

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

PCTF Component Conformance profiles (public versions to be published in their final state at www.diacc.ca) were referenced in their draft state:

- Verified Person Conformance Profile
- Verified Organization Conformance Profile
- Credentials (Relationships & Attributes) Conformance Profile
- Authentication Conformance Profile
- Notice & Consent Conformance Profile
- Privacy Conformance Profile

Government of Canada. GoC Treasury Board Directive on Service and Digital. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32601

Government of Canada. GoC PCTF Public Sector Profile V1.1. https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_1

United States Department of Commerce. National Institute of Standards and Technology. Digital Identity Guidelines (NIST Special Publication 800-63 – 5 documents). 2017. https://pages.nist.gov/800-63-3/sp800-63-3.html

United States Department of Commerce. National Institute of Standards and Technology. Assessing Security and Privacy Controls (NIST Special Publication 800-53). 2014. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

ISACA. Control Objectives for Information Technology (COBIT). www.isaca.org

Axelos. IT Infrastructure Library (ITIL). www.axelos.com

International Standards organization (ISO). Evaluation criteria for IT security. https://www.iso.org/standard/50341.html

US Federal Government, Federal Risk and Authorization Management Program (FedRAMP). See link to document repository. www.fedramp.gov

European Union Agency for Cybersecurity (ENISA). See link to document repository. https://www.enisa.europa.eu/

5. Revision History

Version	Date	Author	Comment
0.01	2019-12-15	PCTF Editing Team	Initial framework draft
0.02	2020-02-14	PCTF Editing Team	Initial content-complete draft
0.03	2020-03-03	PCTF Editing Team	Adjustments based on further research and review of PCTF component drafts
0.04	2020-03-30	PCTF Editing Team	Final adjustments for publication of Draft
0.05	2020-06-05	PCTF Editing Team	Updates based on TFEC member input
0.06	2020-06-29	PCTF Editing Team	Updates as a result of a short supplemental TFEC review period
1.0	2020-07-08	PCTF Editing Team	TFEC approved as Draft Recommendation V1.0
1.1	2020-09-18	PCTF Editing Team	Updates per comments received during Draft Recommendation public review period.
1.0	2020-09-30	PCTF Editing Team	TFEC approved as Candidate for Final Recommendation V1.0
1.1	2022-08-09	PCTF Editor and Infrastructure Design Team	Final Recommendation V1.1 to incorporate alpha testing feedback

1.1	2022-09-14	PCTF Editor and Infrastructure Design Team	TFEC approved as Final Recommendation V1.1