DIGITAL ID AND AUTHENTICATION COUNCIL OF CANADA

Pan-Canadian Trust Framework Overview

A collaborative approach to developing a Pan-Canadian Trust Framework

Authors: DIACC Trust Framework Expert Committee

August 2016

Abstract: The purpose of this document is to describe the background, context, and collaborative approach to develop a Pan-Canadian Trust Framework (PCTF). The PCTF will enable Canada to securely participate in the global digital economy while supporting economic innovation, service delivery, and the principles of an open government.

Table of Contents

Executive Summary

A trust framework is a general term to describe a set of auditable business, technical, and legal rules that apply to the identification, authentication, and authorization of accessing resources across organizations.

This overview introduces the Pan-Canadian Trust Framework (PCTF) collaborative approach. The PCTF enables Canada's full and secure participation in the global digital economy through economic sector innovation and the enablement of modernized digital service delivery. The PCTF supports open government principles.

The PCTF approach builds on global knowledge and experience gained over time and practice. The PCTF is developed through a collaborative approach between the Digital ID and Authentication Council of Canada (DIACC), a non-profit neutral forum, and the Pan-Canadian Identity Management Sub-Committee (IMSC) of the Joint Councils of Canada, a forum consisting of the Public Sector Chief Information Officer Council (PSCIOC) and the Public Sector Service Delivery Council (PSSDC).

Previous work undertaken by the IMSC supports the establishment and communication of trusted digital identities. The identities are anchored in public sector authoritative sources and leveraged by private sector value-added services. Additionally, the PCTF draws on concepts identified in the Principles for Electronic Authentication[1].

The PCTF describes the roles, services, and requirements to be agreed on between participating service delivery and commercial industry sector organizations, to meet current and future Canadian innovation needs. The PCTF leverages the digital identity ecosystem principles listed in this document. Organizations and individuals who wish to participate in the PCTF collaborative development should contact the DIACC.

Background and Context

The DIACC Perspective on Digital Identity Ecosystems[2]

Around the world, governments and industries are developing technology and policy frameworks, more commonly known as trust frameworks. A trust framework enables digital identity and, by extension, facilitates trust worthy digital transactions.

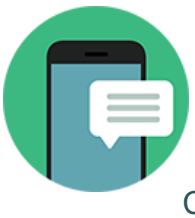
As digital service delivery models mature, governments, businesses, and individuals need to know that personal electronic information is protected as it travels across jurisdictional and organizational boundaries.

Trust frameworks define and standardise processes and practices, and specify data protection policies that government agencies, banks, telecommunication companies, health care providers, and businesses agree to follow with regard to information assurance practices.

[1] Principles for Electronic Authentication, Industry Canada
[2] Building Canada's Digital Identity Future, DIACC

Canada's full participation in the digital transformation and global digital economy depends on developing reliable, secure, scalable, privacy-enhancing, and convenient solutions for digital identity. Made-for-Canada solutions reflect and incorporate Canadian principles, business interests, technical models and, demonstrate compliance with Canadian regulations. Made-for-Canada solutions also enable paths to safe and secure cross-border transactions and service delivery.

The Canadian digital identity ecosystem must be trustworthy, reliable, and enable an individual to securely manage access to their personal information and services. These elements are central principles that underpin made-for-Canada solutions. Canadians expect their digital identification infrastructure to operate with transparency ensuring fairness for all. Furthermore, Canadians expect clear and meaningful notice about why and how their information may be collected and disclosed.



To be truly successful, the use of digital identities must scale beyond a single organization or sector. Digital identities must work within Canada, between sectors, different orders of governments, and internationally. Business processes, systems, and infrastructures need to enable individuals to seamlessly manage their digital identity and personal information across contexts.

Canadians expect clear and meaningful notice about how, by whom and for what purpose their personal information is being used.

It is imperative to create and enable a digital identity ecosystem policy and technology framework that informs the modernization of digital service delivery. Digital economy innovation will enable Canadians to conduct secure, privacy enhancing, and convenient digital interactions domestically and internationally. Canadians must trust that services offered in the the digital identity ecosystem protect and minimize sharing of their personal information. Canadians must understand their right to the privacy, protection, and management of their personal information. Canadians must have access to tools to help them securely manage access to their personal information for specific purposes.

Canadian documents used to identify individuals are being modernized. The Canadian e-passport and the Government of British Columbia's Services Card, a provincially issued smart services card, are two examples of modernized documents. These documents represent physical credentials with electronic capabilities for individuals to digitally identify themselves, anonymously if they so choose, in alignment with Canadian regulations.

Modernized documents increase individual convenience and efficiency while reducing costs for businesses and governments. While modernized documents strengthen the accuracy, security, and privacy protection of transactions, we must enable Canadians to transition to a fully digital-enabled economy where documents and their information can exist securely in the cloud or on their trusted devices.

Requirements of the Canadian Digital Identity Ecosystem

The DIACC proposes 10 requirements of the Canadian digital ecosystem[3]. The DIACC recognizes that additional principles may be identified and considered with respect to specified service delivery and economic sector needs, such as the Principles for Electronic Authentication published by Innovation, Science, and Economic Development Canada (formerly Industry Canada) in 2004[4].

[3] Building Canada's Digital Identity Future, DIACC
[4] Principles for Electronic Authentication, Industry Canada

1. Robust, secure, scalable;

Canada's digital identity ecosystem must be robust enough to ensure it is secure, available, and accessible at all times. Full time services access also requires redundancy and disaster recovery tools.

The ecosystem infrastructure must enable the digital services delivery and economic sectors to adopt the latest advances in security technologies and policies. Protecting personal information is a non-negotiable priority. Infrastructure design must secure personal information that is both in transit and at rest. Infrastructure must rely on a foundation of awareness and training for expertise including: access control, audit and accountability, risk assessment, penetration testing, and vulnerability management.

A trust framework that governs digital identity ecosystem solutions and services must scale to securely enable innovation. Some entities are ready to accept digital identities while others are not. A digital identity ecosystem trust framework must be designed to enable the service delivery and economic sectors to integrate at scale.

2. Implement, protect, and enhance Privacy by Design;

Digital privacy enhancing tools enable an individual to manage who may access their personal information for a specified purpose. DIACC members focus on the identification and development of tools and policy that respect Privacy by Design as a foundational element of digital identity interactions. Solutions need to be able to prove compliance with applicable Canadian data protection laws and regulations.

3. Transparent in governance and operation;

Canadians need to trust that services offered in the Canadian digital identity ecosystem will respect and meet their needs. Canadians need to have trust in the policies and practices that govern the Canadian digital identity ecosystem. It is critical that Canadians have transparency and opportunities to engage with experts who influence policy and technology regarding the governance of their digital identity ecosystem.

4. Inclusive, open, and meets broad stakeholder needs;

Digital identity ecosystem services and tools must be affordable, standardised, and beneficial to Canadians. Services must be secure and innovative while reducing economic costs of operation. A trust framework must be flexible enough to enable established and innovative technologies and services. The ecosystem must be beneficial to individuals as well as to commercial service and technology providers by mitigating risks while enabling opportunities to develop sources of revenue.

Business and public sector entities share the need to deliver secure modernized digital services to their constituents while minimizing costs. Individuals must have equal and convenient access to services regardless of geographic location. All Canadians must be able to understand and use services offered in the Canadian digital identity ecosystem, regardless of their personal abilities[5].

All Canadians must be able to easily understand and use services offered in the Canadian digital identity ecosystem, regardless of their personal abilities.

5. Provides Canadians choice, control, and convenience;

Privacy respecting and enhancing services rely on the principle that individuals are informed about the details and potential benefits and consequences

[5] Principles for Electronic Authentication, Industry Canada

associated with personal information management. Informed individuals are likely to make better decisions about how their personal information is provided, shared, and used.

Informed consent requires that individuals have a clear understanding of the facts, implications, and potential consequences of an action. Informed consent is gained by providing an individual with the knowledge and tools to securely manage access to their personal information.

Digital identity ecosystem services and tools must be easy to use. Remembering dozens of passwords or carrying 15 different cards is not a scalable or secure approach. If an individual forgets their password (or other identifier) or loses their identification (or device upon which it is stored) they must be able to securely and conveniently re-validate their digital identity with ecosystem services. Digital identity ecosystem services must be secure enough to prevent fraud and convenient enough to allow for rapid authentication and access control.

Users need the ability to use their digital identity securely and conveniently.

6. Built on open standards-based protocol;

Use of open standards and applicable best practices for Canada's digital identity ecosystem will help protect against obsolescence, ensure interoperability, and foster a dynamic and competitive solutions market environment. Building Canada's digital identity ecosystem on open standards-based protocols will ensure that Canadians are not locked into one technology or supplier. The risks of governments and companies being locked into closed ecosystems must be mitigated.

Adoption of an open standards based approach allows different services, based on standards driven technologies, to seamlessly connect. This is essential to allow the digital service delivery and economic commercial sectors to leverage interoperable and verifiable solutions that best meet their needs.

7. Interoperable with international standards;

Interoperability and global technology and policy standardizations are foundational to todays connected world. Much like standardised railway gauges enable travel and the transfer of goods across countries, and the standardisation of cargo container sizes reduces shipping costs, technology and policy interoperability and standardisation allows digital services to communicate and lower costs while increasing innovation opportunities. For Canada to thrive in the global digital economy, we need to ensure that our digital identity ecosystem is able to interact with information systems around the world while respecting our own cultural, constitutional, legislative, and regulatory needs.

For Canada to thrive in the global digital economy, we need to ensure that our digital identity ecosystem is able to interact with systems around the world…

8. Cost effective and open to competitive market forces;

It is essential that the digital identity ecosystem respects the budgetary constraints of the present and the future. Ensuring the ecosystem is open to competition, representing multiple economic sectors, each playing different roles, will lead to decreased costs for individuals and increased innovation.

9. Able to be independently assessed, audited, and subject to enforcement;

For Canadians to trust a digital identity ecosystem, governing controls must be put in place. On-going, functionally independent, and third party, assessments provide one way to ensure that ecosystem entities and services are adhering to the trust framework requirements. Services demonstrating compliance may leverage a trust mark, while services are not in compliance will not be seen as trustworthy and will not leverage the benefits of the trusted digital identity ecosystem. Where possible, the PCTF will reference internationally adopted technology and policy standardisations. That said, PCTF participating entities and services are subject to applicable Canadian laws and codes for operations within Canadian jurisdictions.

Functionally independent, and third party, assessments provide one way to ensure that ecosystem entities and services are adhering to a digital identity ecosystem trust framework.

10. Minimizes data transfer between authoritative sources and will not create new identity databases

Users of digital identity ecosystem services should be asked to provide only the minimum amount of personal information necessary to complete an interaction. Where possible, and appropriate, anonymous transactions should be supported. This is critical, if Canada is to embrace an ecosystem in which people engage in activities such as e-voting.

Trust Frameworks – An Overview

A trust framework consists of a set of agreed definitions, requirements, standards, specifications, processes and criteria. The set of agreed details enable identity management process and authorization decisions carried out by other organizations and jurisdictions to be relied on with a standardised level of confidence. Simply put, a trust framework enables one organization to rely on a business or technical process carried out by another organization with confidence.

A trust framework is intended to help define and enable innovative solutions that can be offered across the country. The trust framework is not intended to impose or constrain design or technology decisions. Rather, a trust framework helps situate how new and existing solutions can work together in a standardised and trusted manner.

A trust framework is intended to be understood by a wide range of stakeholders, and be clear enough to be adopted and consistently applied by many different communities, service providers and practitioners. Finally, and most importantly, a trust framework is intended to be a key enabler to the larger digital economy. If done correctly, a trust framework is invisible to those who rely on it every day - individuals and businesses conducting digital transactions with the knowledge that trust underlies everything that they do.

Trust frameworks enable better services and digital transactions by ensuring the consistent identification of individuals and organizations. Trust frameworks ensure consistency of interactions between institutions, businesses, and individuals when dealing with identification, authentication, and authorization.

Trust frameworks are used by a community with shared interest to increase the experience of predictability and transparency and manage risk when using services within that particular

community. Trust framework components identify, define, and specify common processes and expectations of entities participating in the digital community.

Trust Framework Purposes

The term trust framework commonly describes several types of uses for varying purposes and concerns.

Purpose	Concern
Access Federation	Reliable issuance of credentials, assignment of permissions and access control policies, technical specification and audit.
Digital Identity Federation	Establishment of identity information, 'binding' identity records to credentials, protection of privacy, technical interoperability.
Technical interoperability	To define the specifications and profiles of standards to allow multiple systems to interact and exchange information reliably.
Policy interoperability	To establish compatible policies between organizations to support predictable outcomes between and within organizations.
Legal administration	Trust framework standardisation of common terms, expectations, and defined processes enables efficient model contract and agreement development. While entity contracts and agreements are informed by a trust framework, specific agreements and contracts are not themselves part of the trust framework.

The Pan-Canadian Trust Framework

The PCTF is a key underpinning to ensure that the Canadian digital identity ecosystem is trustworthy and encourages a fair, innovative, and competitive environment. Furthermore, the emerging digital identity ecosystem is at country-scale, and therefore in scope, the PCTF supports the inclusion of participants offering of broad range of services for both the digital service delivery and economic sectors.

The PCTF provides business value for a diverse array of participants that is commensurate with risk and takes into account the different perspectives of public sector and private sector stakeholders:

- **For individuals or organizations (as end users of services):** The PCTF increases confidence in the protection, disclosure, and use of their identity and personal information, thereby enabling a "tell us once" approach for convenient access to services in a trusted, secure, and privacy-enhanced manner.
- **For governments, institutions, and businesses:** The PCTF provides an opportunity to offer standardised, high value, high integrity services between jurisdictions and the private sector. The PCTF also provides an opportunity to rely on many trusted service providers, which improves the overall integrity, efficiency and streamlining of high value and complex digital services.

Intended Audience, Application and Authority

The PCTF is intended to be applied across industries and subject to Canadian laws and regulations. The PCTF will enable an ecosystem of trusted services as a trusted foundation for digital interactions. The PCTF assists designers, builders, and providers of online standards-based identification, authentication, and authorization systems and those wishing to rely on and trust established digital identities. Specific and applicable authority and governance of the participating entity services will be developed through collaborative efforts and will be published in future specified documentation.

Pan-Canadian Trust Framework Scope

The PCTF leverages the outputs and previous accomplishments of the IMSC through collaboration with the Canadian economic sector. The PCTF develops mechanisms for digital identity ecosystem participants to interact with integrity based on common terminology, concepts and technical specifications. The PCTF is designed to be suitable for digital identification, electronic authentication, online credential, and authorization systems used to provide services to government entities, citizens, business partners, and customers.

The PCTF extends the output and previous accomplishments of the IMSC through collaboration with the Canadian economic sector to describe mechanisms for digital identity ecosystem participants to interact with integrity…

Canadian citizens and consumers, i.e. end users, are the ultimate beneficiaries of trust that is achieved through service standardisation and accountability to the PCTF. The intended participants and implementers of the PCTF are government, commercial, non-profit, and other entities who offer and consume identity services in support of their business and program activities.

The PCTF exists to enable the Canadian digital identity ecosystem and will be used to identify applicable existing policy and technology standards that meet the needs defined in the PCTF. The PCTF may be used to identify future areas for collaboration, development, and standardisation.

Pan-Canadian Trust Framework Value

The PCTF can provide value in the following areas:

- Represents the considerations of Canadian public and private sector principles with regard to service delivery and full participation in the global digital economy;
- Defines Canadian digital identity ecosystem standardised roles, rights and responsibilities;
- Describes operational practices expected of participants in order to manage interaction risks;
- Enables the owners of resources to better understand the opportunities and liabilities when providing access to or allowing the use of resources;
- Recognizes the contexts, unique and common requirements of public and private organizations;
- Is structured to be responsive to future government and industry requirements; and
- Defines common ground for an ecosystem of digital identity producers and consumers in support of gaining authorized access to online services.

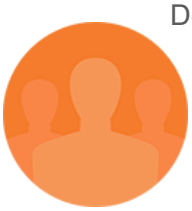
Through a collaborative effort of the Canadian digital service delivery and economic sectors, the PCTF represents the set of agreed business, policy, and technical requirements, specifications, standards, policies, procedures, and assessment criteria. The PCTF also establishes participation requirements, rules, and tools that allow partner organizations to come to agreements more quickly by leveraging a common understanding of definitions, specifications, and multi-lateral, or centralized federation agreements.

Pan-Canadian Trust Framework Structure

The PCTF will consist of related documents including:

- Overview
- Glossary
- Trust Framework Components and Conformance Criteria Core
- Technology and Policy Interoperability Criteria Profiles
- Supplemental Governance and Instructional Processes

Conclusion



Development of the PCTF is a collaborative initiative between the DIACC and the IMSC of the Joint Councils of Canada, a forum consisting of the Public Sector Chief Information Officer Council (PSCIOC) and the Public Sector Service Delivery Council (PSSDC). The PCTF enables the delivery of innovative, secure, privacy-respecting, and convenient solutions to all Canadians for modernized service delivery and to ensure Canada's full and beneficial participation in the global digital economy.

The DIACC is a non-profit neutral forum established to identify and develop standardisations and innovations that support trustworthy digital identity based interactions for the economic and societal benefit of Canada.

Previous work undertaken by the IMSC supports the establishment and communication of trusted digital identities, anchored in authoritative sources. The PCTF extends the output and previous accomplishments of the IMSC by describing mechanisms for other digital identity ecosystem participants to interact with common terminology, concepts and specifications.

As the development of the PCTF progresses, the DIACC community will implement a plan to consult with the broader public to gather input for consideration. The DIACC is a non-profit neutral forum established to identify and develop standardisations and innovations that support trustworthy digital identity based interactions for the economic and societal benefit of Canada. Entities and organizations who wish to participate in these collaborative efforts should contact the DIACC for further information.

About the DIACC

Created as a result of the federal government's Task Force for the Payments System Review, the DIACC is a technology agnostic non-profit coalition of public and private sector leaders committed to developing a Canadian digital identification and authentication framework to enable Canada's full and secure participation the global digital economy.

The DIACC's objective is to unlock economic and societal opportunities that benefit Canadian citizens, consumers, and businesses by accelerating the development of a robust, secure, scalable and privacy enhancing digital identification and authentication ecosystem that will decrease costs for governments, consumers, and business while improving service delivery and driving GDP growth.

DIACC's members share resources by working together to identify and develop industry standards, research, and proofs of concepts that address policy, business, legal, and technical requirements for the interoperability and adoption of trusted digital identity services. DIACC invites entities and organizations in Canada and globally to participate in the efforts. Interested parties are invited to browse diacc.ca and to contact us for further details.