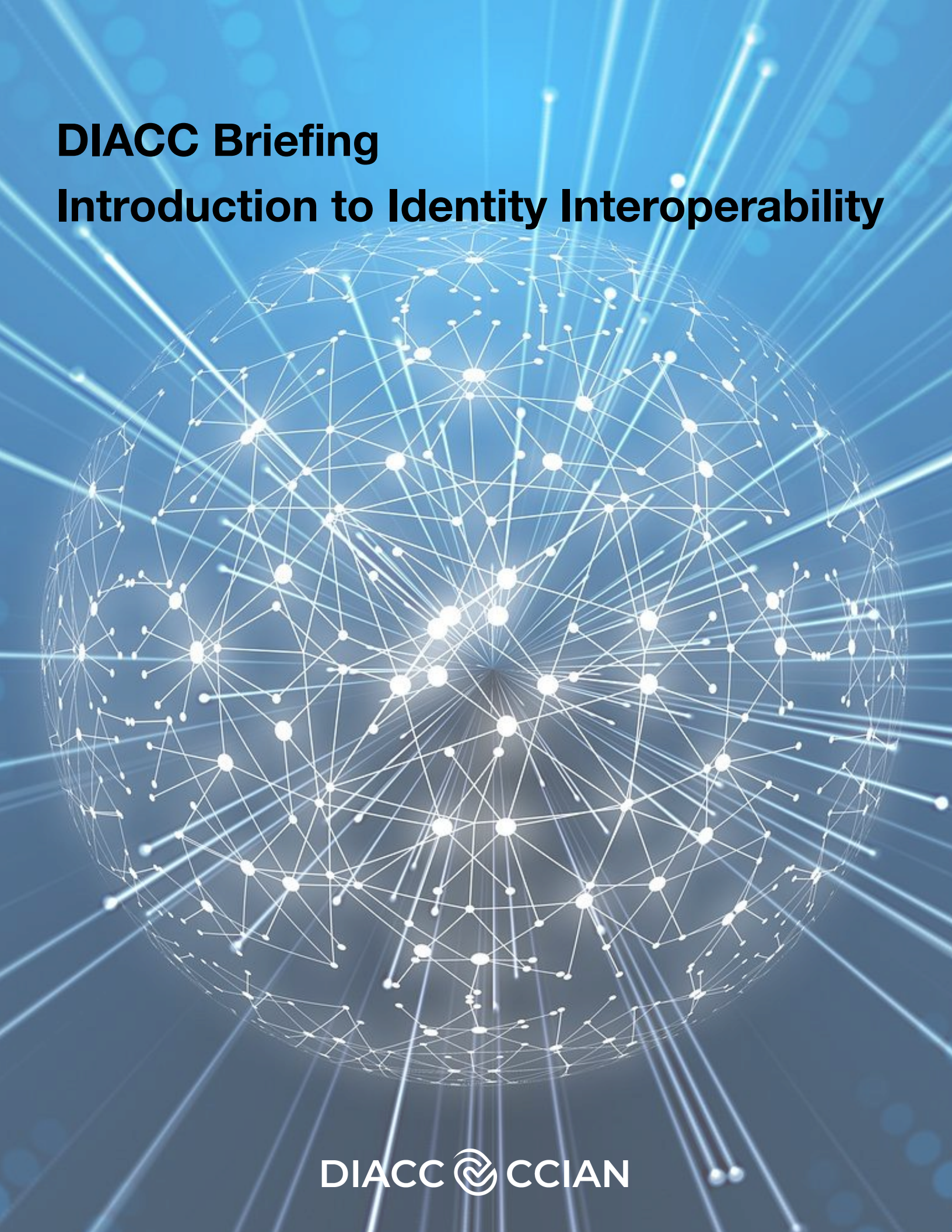
DIACC Briefing

Introduction to Identity Interoperability



DIACC CCIAN

Table of Contents

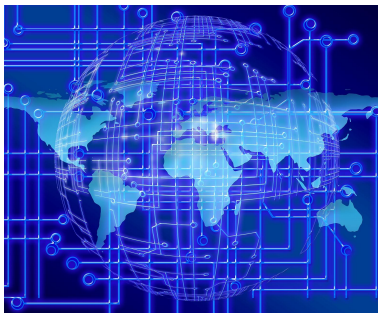
About the DIACC

Created as a result of the federal government's Task Force for the Payments System Review, the Digital ID & Authentication Council of Canada (DIACC) is a non-profit coalition of public and private sector leaders who are committed to developing research and tools to enable secure, robust, and scalable Canadian digital ID solutions and services. With privacy, security, and choice at the forefront of all DIACC initiatives, the DIACC aims to enable all Canadians to participate safely and confidently in the global digital economy.

Contributors

The content herein has been developed with contributions from members of the DIACC's Innovation Expert Committee including Consult Hyperion, the Digital Identity Laboratory of Canada, Autorité Des Marchés Financiers, Northern Block, Stonebridge Solutions, and Vaultie with additional support by Accenture and Outlier Solutions.

Executive Summary



Interoperability is crucial for developing efficient, sustainable, secure, and useful identity ecosystems. Identity interoperability is the ability to share identity standards, frameworks, or protocols between identity systems or models to allow computer systems or software to exchange and use identity information within and across organizational, regional, and national boundaries. Assurance frameworks in particular, like the Pan-Canadian Trust Framework (PCTF), help to establish an expected baseline and frame of reference for both public and private sector digital identity capabilities while prioritizing user-centered design, privacy, security, and convenience of use.

Additionally, it enables the development of more efficient and sustainable identity systems with long-term potential by allowing organizations to share data and resources, thus reducing development and operating costs. Technically, interoperability is the ability of different functional units (e.g., systems, databases, devices, or applications) to communicate, execute programs, or transfer data in a manner that does not require the end user to have an in-depth knowledge of those functional units (ISO/IEC 2382). (source: Interoperability | Identification for Development).

Identity interoperability improves both the end-user experience and the safety of personal data by minimizing the need to duplicate identity data circulating on public networks. This, in turn, reduces the number of potential points of failure and combined with the more sophisticated identity verification processes that interoperability allows, it significantly increases security and reduces the risk of identity fraud.

Furthermore, interoperability generates value for the end users, enabling the use of their verified digital identity in a more versatile way by providing access to various services and platforms, like digital government, digital commerce, digital health, and others. This improves accessibility and reduces barriers for citizens who may not have access to traditional forms of identification.

In short, interoperability plays a crucial role in developing efficient, sustainable, secure, and useful identity ecosystems by enabling the context-appropriate sharing of data, improving identity verification, reducing costs, and improving accessibility.

Introduction: The Purpose of Identity Interoperability

Previous papers published by the DIACC have explored a variety of concepts[1], guidelines[2], policies[3], products[4], and frameworks[5] that are all working in parallel to guide the advancement of digital identity and digital trust services across the digital economy. The DIACC and its members share a common goal and mission that envisions a future where the way people, businesses, and governments interact with each other in a digital context, and through digital transactions, can and will be significantly changed for the better of all ecosystem participants through the benefits of widespread digital identity.

The general purpose of interoperability is to enable different systems, technologies, and organizations to work together coherently and exchange information. This collaborative process allows for an efficient and secure sharing of data, while improving the user experience through reduced friction, and increasing the overall functionality and utility of the systems. In the context of digital identity, interoperability means a user can use a single identity across multiple services and platforms, without the need to duplicate usernames and passwords for each of them. Less duplication reduces the number of potential points of failure, and consequently, interoperability improves security while also making it less challenging for individuals to access different services and platforms.

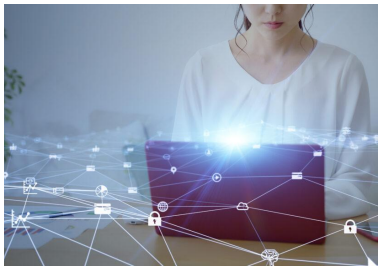
Through verification processes, identity interoperability allows for the implementation of more sophisticated ways to verify identity, enabling collaborating organizations to verify and share identity information in real-time. This allows for an increase in security and a reduction in the risk of identity fraud.

Interoperability enables the development of more efficient and sustainable identity systems. The shared standards, frameworks, and protocols allow participating organizations to put in common useful data and resources, reducing the need for redundant systems and lowering the costs of required identification processes.

---

[1] Making Sense of Identity Networks (2020)
[2] Making Sense of Digital Wallets (2020)
[3] Policy design principles to maximize people-centered benefits of digital identity (2022)
[4] Directory of Products That Assess Identification Documents and Verify Identity (2021)
[5] Decentralized Identity and DIACC PCTF Authentication (2021)

Lastly, identity interoperability creates significant value for the end user, as it allows for the use of digital identity in a more versatile way. It has the potential to provide access to various services and platforms (such as digital government, digital commerce, digital health, and others) with a verified digital identity, according to that organization's acceptable level of risk. If implemented correctly, this approach can also have positive impacts on accessibility and reduce barriers for citizens who may not have access to traditional forms of identification.



In short, the primary purpose of identity interoperability is to enable different systems, technologies, and organizations to work together seamlessly and exchange identity information, and collaborate in the identification process to improve the user experience, increase security, reduce costs, and improve accessibility.

"Interoperability and compatibility are essential to the adoption and realizable value of digital identity programs, and the emergence of new standards is a key enabler.[6]"

As was explored in depth within the Making Sense of Identity Networks paper, there are established problems with the way digital transactions and interactions are conducted today:

"Today, identity is often siloed, with customers needing to have separate relationships with each organization they deal with and each organization keeping a separate (and likely different) digital version of the customer. This creates massive friction and risk. Without reliable and portable digital identity, consumers, governments, and businesses will have a significant lack of trust in online interactions, which in turn will prevent everyone from fully realizing the full potential of digital services."

The lack of trust in digital services and online interactions is currently fueled by the fact that the internet as it stands today is not as safe, secure, trustworthy, or reliable as it could be across many contexts. Not only can the internet be difficult for some people to access or use, but it is also full of fraudsters wanting to steal information and money, and when anything significant changes (e.g., you move, you get a new phone, you forget your password) getting back up and running can be both time consuming and frustrating. Considering this reality, identity

[6] Policy design principles to maximize people-centered benefits of digital identity (2022)

interoperability is indeed a key enabler to unlocking the full potential and value that online digital processes can provide.

Defining Identity Interoperability

Each one of the papers mentioned above in some way describes or references the concept of interoperability yet does not explore this topic in any depth. While the notion of "interoperability" may have initially been intended to refer to interoperability between technologies or software systems, in the context of digital identity we are considering a broader definition. To understand identity interoperability, one must assume that a subject (a unique individual, organization, or device distinguishable from others), needs to either go through or have previously gone through the process of identification (to establish a real, unique, and identifiable subject), with a particular service provider or identity network.

A simplified definition of identity interoperability is to facilitate organized and effective identity data exchange between different systems, devices, applications, or products to connect and communicate in a coordinated way, without effort from the end user, allowing him to use a single unique identity to connect to any of those systems, devices, applications or products.

There are fundamental human purposes beyond the technologies, policies, standards, and frameworks necessary that support interoperability which must be acknowledged:

- First, is the ability for an individual to assert their own identity digitally;
- Second, the individual and other stakeholders trust that the assertion is reliable;
- And third, their digital identity is protected and accepted wherever and whenever they choose to present it.

The interoperability of identity must contemplate a broad range of current and future digital identity ecosystems and approaches while staying compliant with emerging regulations and maturing global standards and frameworks. Interoperability efforts also need to be flexible enough to support constantly evolving connections and innovation within the relevant digital identity ecosystem.

Layers of Interoperability

To better understand the inner workings of identity interoperability, we must appreciate how such collaboration can be deployed between multiple users and organizations. Even though the desire to achieve interoperability between identity ecosystems across the digital economy can be strong, the process is not as easy as it may sound or as simple as is sometimes suggested.

Reaching functional interoperability is a complicated process and can be broken into several distinct focus areas that we consider interoperability layers. Technical standards, frameworks, specifications, and governance define how interoperation between components can be achieved to create a secure environment allowing the transfer of identity information. The focus areas through which interoperability can be reached are as follows. They do not only pertain to identity interoperability but are nonetheless the building blocks of interoperable processes:

1. **Legal Interoperability** - the required governance for enabling the lawful acceptance, processing, or storing of any data exchanged within the context of a transaction.
2. **Organizational Interoperability** - the alignment of business processes, responsibilities, and expectations to achieve commonly agreed and mutually beneficial goals.
3. **Semantic Interoperability** - the ability of two or more systems to exchange relevant data without requiring a rigid interface standard or shared programming language.
4. **Technical Interoperability** - the capacity of different systems, devices, applications, or products to connect and communicate together in a coordinated way, without any effort (or even awareness) from the end user.

As one can appreciate from those interoperability building blocks, deploying each layer properly to enable interoperable identity ecosystems is a challenge, requiring efforts from a wide range of participants across the digital economy. But the end goal, as a community, is to reach an agreement on common approaches in order to enable a journey as seamless as possible for the collective end users. If that goal is pursued and reached, the value created by, and for everyone involved, will be well worth it. Identity interoperability is only one piece of the digital identity puzzle, albeit a significant one. It has the potential to change the way digital transactions are happening today and to open up new opportunities or use cases that were not previously possible (or even considered).

Note: The layers of interoperability as described above have been simplified for an easier explanation of the concepts. The DIACC envisions developing additional content to explore these topics in more depth than is possible in this executive briefing.

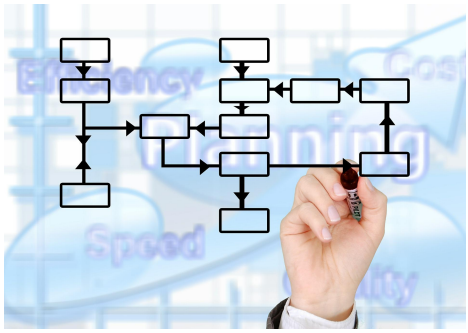
Value of Interoperability

As described in the previous section, each layer provides specific benefits to ecosystem participants, and those benefits become cumulative when multiple layers are combined. This means that interoperability has the potential to generate significant benefits for every stakeholder participating in a digital identity ecosystem. Those benefits, that we can consider as the intrinsic value that identity interoperability can provide to organizations, are realized across several key areas including streamlined business processes, reduction of data duplication, enabling a risk-based approach to their processes, and through the value of global open standards.

Streamlined Business Processes

Interoperability can help streamline business processes, allowing for faster and more efficient service delivery. As presented earlier, in essence, interoperability is agreeing to a set of standards, which positively impacts both the service provider and the end user, making transactions easier, and allowing a higher volume to be processed in a simpler and faster manner.

From the end user's, or subject's point of view, interoperability can increase trust in the digital process and reduce friction. For example, if the subject has an existing relationship with a trusted identity provider, and this provider is part of an interoperability group (network), we can assume that the subject's trust (and, consequently, use) with any participants of the group will legitimately increase.



From the service provider's point of view, interoperability can increase efficiency and therefore, decrease delivery time without increasing the risk of errors. Having both customers and business partners agree on a set of standards will allow the service provider to focus its efforts and resources where the process added value is, instead of spending them to define an identification process from scratch. The risk of mistakes or errors is therefore reduced as implemented interoperability standards allow seamless information transfer without the need for human interaction.

Consequently, this will speed up the service delivery time as less efforts will be required by the clerical aspects of the transaction. The impact of this is that interoperability has the potential to:

1. Reduce time and effort spent while not generating value to the end user
2. Reduce mistakes and errors
3. Speed up service delivery time

Finally, from the identity provider perspective, interoperability can create additional value out of available data and existing processes in the organization. As it is safe to assume most identity providers have a desire to foster a wide and durable relationship with their customers, the value that can be created through interoperability can go further than the monetary aspect (for a non-governmental/private identity provider). Interoperability can increase the frequency and volume of transactions with its customer (customer "stickiness"), benefit customer lifetime value, and increase customer satisfaction while providing them with a seamless, fluid, and satisfying user experience. From a public sector perspective, those same benefits can potentially increase both the democratic involvement of the end user, and the broad appeal of the provider's program to the general population.

Reduction of Data Duplication

So if the basis of identity interoperability is to agree on a shared set of standards and frameworks, then the operationalization of it relies on a shared identity dataset (through an identity network, for example). This approach to shared identity data reduces data duplication (identity interoperability aims to eliminate the need to create a "new" identity for each new service provider), and will improve identity data integrity while at the same time decreasing the risk of fraud or data theft, by reducing both the potential vectors of attack and the surface area available to them.

Enabling a Risk-Based Approach

Data can, without a doubt, be exchanged securely through shared technical protocols supporting identity interoperability. In such a secure environment, participants will adapt the way they interact to their operational needs, based on the intrinsic characteristics of the interoperability network architecture that is used.

Each stakeholder will be adopting a risk-based approach, looking to minimize the risk throughout their own processes and using interoperability to streamline their identification

process. This approach to shared digital identity can contribute to minimizing a risk profile, for example by using security-by-design as a strategy, or by eliminating the exchange of identity data irrelevant to the transaction.

Global Open Standards and Frameworks

A cooperative distribution model and adoption are key success factors for the deployment of functional identity interoperability. This model allows a more neutral and independent approach to technology and protocols, opening the door to global open standards and frameworks. As seen in similar global efforts (e.g. the Australian Trusted Digital Identity Framework [TDIF]), this can also foster a baseline security benefit for solutions that demonstrate interoperability, in particular defining for those that are not subject-matter experts what a good identity system looks like.

Our premise is also that open standards and frameworks benefit every stakeholder, whichever role they have in an identification process. They allow everyone to move in the same direction of mutual value creation while fostering innovation and evolving with the best practices in the field. We could compare the open standards and frameworks approach to a rowing ship, with everyone rowing in the same direction, with the same rhythm: it will surely propel the boat forward and allow it to reach its destination sooner.

Conclusion

Interoperability is truly vital to developing and maintaining efficient, sustainable, secure, and useful identity ecosystems. The benefits can be substantial for all those involved by improving end-user experiences, decreasing administrative inefficiencies, improving the integrity of identity data, mitigating risks, reducing fraud, and promoting technology and vendor neutrality. Interoperable identity ecosystems put the power and control of a person's identity information in their own hands, ensuring they can choose how and with whom to transact digitally in a way that is both safe and convenient. Assurance frameworks in particular (like the PCTF) help to

establish an expected baseline and frame of reference for both public and private sector digital identity capabilities while prioritizing user-centered design, privacy, security, and convenience of use.

As Canadians are becoming more reliant on digital technology to connect, work, and access services, it's crucial that we encourage the establishment and implementation of trusted interoperable identity systems.