DIACC

BUILDING CANADA'S DIGITAL IDENTITY FUTURE

A REPORT BY THE

DIGITAL IDENTIFICATION AND AUTHENTICATION COUNCIL OF CANADA

MAY 2015

A compelling need for change

Canadians are rapidly adapting to life in the digital age.

We shop online. We bank online. We access government services online. We are enthusiastically adopting all manner of digital technologies and services to improve how we work and live. Mobile devices, mobile apps and cloud-based services are just a few recent developments that promise to transform the way entire industries do business. In many cases, they already have.

Inevitably, we are asking: Why we can't do more online? Why can't we go online to access medical records, sign contracts, or apply for a passport? Canadian taxpayers will pay an estimated $376 million[1] for the 2015 federal election despite the prospect of a smaller voter turnout. Why can't we vote from home? Maybe that's too much to imagine right now. But why is it that we can pay for our children's hockey camp online yet have to print off and sign a physical copy of the liability waiver?

The answer is simple. These systems don't know who we are with enough confidence to provide the services we want. Despite the digital transformation going on around us, the methods of proving our identity remain locked in a traditional physical mode, with paper or plastic documents. The reliance on traditional modes of proving identification and authentication is becoming a significant barrier to innovation.

To be sure, broaching the topic of digital identity is difficult. But it has also never been easier to move this discussion forward. True, headlines are full of revelations that systems have been breached and private information is less secure than we'd expected by now. But it is also true that today, organizations large and small face the same imperative to imagine a smarter way to store and access our data.

Several governments around the world are tackling this challenge by rolling out new centralized national ID systems with digital and biometric components such as iris scanning and fingerprinting. There is little appetite for a new national ID in Canada. Canada is a federal parliamentary system in which governance is divided between a central government and distinct member governments in the provinces and territories. Similarly, our traditional identity systems are federated—generally rooted centrally in passports and social insurance numbers and, in the provinces, in more commonly used registries of birth and death, driver's licenses, and health cards.

A new digital identity system will allow us to do things online that we have traditionally used physical ID for in person. Preferably, the new system will also be useful for in-person based processes. It must allow for federation, preferably across both the public and private sectors since, in our everyday lives, we are much more likely to use our banking credentials than our passports. It must be robust, secure, scalable and provide no additional risk to personal information and privacy. It must also be privacy enhancing.

This is a complex and costly undertaking—a task so complex and varied that it does not fully exist yet. Banks and other large commercial establishments can afford to build digital identification systems for their own customers. But what about using this identity to access school records? What about hockey camp? As a society we are waiting for a leader to step forward and create the digital ecosystem of the future. While we wait, institutions are building point-to-point solutions that are complex, limited

[1] See: http://bit.ly/1ySWnjS

and difficult for the user, and that introduce inconsistencies into an ecosystem that we know should be uniform in order to encourage adoption and security.

Both the public and private sectors are realizing the scale of the problem and that we must work together to solve it. Canada Health Infoway has recently published its Federated Identity Management in Health Care White Paper.[2] The Joint Councils of Federal, Provincial and Territorial Governments have developed the Pan Canadian Assurance Model[3] and the Pan-Canadian Identity Validation Standard,[4] and are now working on a Pan-Canadian Identity Trust Framework. The Government of Canada, in collaboration with the provinces and territories, is leading Canada's Digital Interchange, a strategic initiative for enabling cost-effective ways to securely confirm an individual's identity information. Many organizations within the private sector have made great strides to address the challenges. But a concerted, coordinated effort across all sectors is required.

Canada could do more

Some Canadian documents used to identify individuals are being modernized. The Canadian e-passport and the BC Services Card, a provincially issued smart services card, are important developments. These modern documents represent the next big step: physical cards with embedded electronic capabilities that provide secure ways for people to electronically identify themselves if they choose to do so, all within the bounds of Canadian regulations.

These documents represent a great step toward digital identity; they improve the accuracy and security of our transactions. They can be used online to gain greater efficiency and lower costs for businesses and governments and provide greater convenience and privacy for Canadians.

But Canada could do more.

It is no exaggeration that Canada's economic future absolutely depends on developing a reliable, secure, scalable, privacy enhancing and convenient solution for digital identity. To be truly successful, digital identity must scale beyond a single organization or sector; it must extend beyond jurisdictions and work anywhere within Canada, between sectors and different orders of governments, and internationally. To support this, we need to build systems and infrastructure that place the individual in control of their digital identity in a way that is seamless across boundaries.

Around the world, governments and industry are developing frameworks and policies to enable digital identity and, by extension, facilitate digital transactions. The UK government recently launched GOV.UK Verify, which enables users to prove who they are online as they access government services. Estonia has already developed secure networks that enable users to digitally access more than 3,000 services, including voting, health records, even school homework and the purchase of bus fares.

Countries are developing "trust frameworks," which are certification programs that allow parties to trust each other's identity, security and privacy policies. In the U.S., a public-private partnership called the IDESG (IDentity Ecosystem Steering Group) has established the Trust Framework and Trustmark Committee. The European Union, as part of its Digital Agenda, has passed the *Electronic Identification and Trust Services Regulation*. These frameworks and regulations

[2] See: http://bit.ly/1HqYqik

[3] See: http://bit.ly/1DEmzuz

[4] See: http://bit.ly/1DmEPJD

are defining and standardizing identity proofing, security and privacy requirements that everyone must follow. In some cases, these frameworks and regulations specify the data protection policies that government agencies, banks, telcos, health care providers and other businesses must follow to reach a specific level of designation.

In the absence of a robust digital identity ecosystem, the private sector leads the way forward by default. History has shown several examples of private-sector led identity initiatives that have not always acted in the best interests of the public. Millions of people use services such as Facebook, Google or Twitter to login to other services or websites. Some sites no longer let you create credentials but instead force you to logon to Facebook to connect. While this may be convenient, it is not clear that all users understand the implications of using such a login service. For example, what data is shared between the services and Facebook? Where else, and how could a user's activities be shared? Google's terms of use give the company permission to use what it knows about a user's online activities (a lot) for a wide range of purposes. This can be very beneficial and convenient—for instance, recommending a restaurant you might like in an unfamiliar town or alerting you to sales at your favourite stores. However, there is also the potential for this information to be used for purposes that are not always in the user's best interest, such as sharing health care information, or sharing personal habits with prospective employers or insurers.

Let's build a digital identity ecosystem worthy of our trust

In Canada, the jurisdiction of identity is a responsibility separated between the federal, provincial and territorial governments. The traditional approach has been to work independently within each jurisdiction, but this is changing. Digital identity requires a collaborative, pan-Canadian approach that is interoperable with different systems be they federal, provincial, territorial or private sector. The need to work together is no longer a "nice-to-have" but rather a core requirement as Canada transitions into a fully digitally enabled economy.

The Digital Identification and Authentication Council of Canada (DIACC) believes it is imperative that Canadian institutions protect and promote Canadian values and perspectives as the digital economy develops. If we do not, Canadians will be followers rather than leaders. We will be forced to adopt standards that may not reflect what we value as Canadians.

It is imperative that we promote and develop a robust, secure, scalable and privacy-enhancing, made-for-Canada digital identification ecosystem that serves as the backbone for Canadians to conduct a wide range of secure online transactions and interactions, domestically and internationally. For such an ecosystem to flourish, Canadians must be willing to adopt it. To adopt it, Canadians must trust that the ecosystem will protect their private information, and that we will have greater control over how much and when we share our personal information, with whom and for what purpose. We need to control how long it will be stored and what our future rights are with respect to our data.

Without question, Canada can do this. We have the proven technical prowess, the industrial expertise and the requisite trust in government institutions to build an ecosystem Canadians will embrace. But no single government or private enterprise can do it alone. We need a concerted and co-ordinated effort between the federal and provincial governments, as well as the private sector, to build an ecosystem that will allow us all to safely, securely, conveniently and profitably conduct transactions in a digital world.

DIACC calls on federal, provincial and territorial governments and the private sector to do the following:

1. **Propel digital identity programs and projects forward** by building upon:
    a. our strategic advantages (Digital Canada 150),
    b. world leading expertise (DIACC, IdentityNorth, Canadian technology companies),
    c. historical leadership in the realm of privacy (Privacy by Design, 7 Laws of Identity), and
    d. recent successes (the Government of Canada's Sign In Partner Credentials).
2. Develop a sustainable business and operating platform, and **deliver or support delivery of a live commercial service for digital identification and authentication** by a specific date.
3. Adopt a **Federated Authentication and Brokered Authorization Model** as a pan-Canadian standard for a robust digital identification and authentication regime, with privacy at its core.
4. Identify requirements and **develop standards** and trust framework(s) to support the business and technical models for a robust digital identification and authentication regime, with privacy at its core.
5. Address the need for **legislative and regulatory change** to recognize and accept digital identification.
6. Build grassroots support for this enterprise by **educating Canadians** and recruiting stakeholders across all industries and sectors.
7. **Develop an industry trust mark** to provide confidence in the marketplace

The Government of Canada's Digital Canada 150 strategy[5] and the Federal Provincial Territorial (FPT) Identity Management Sub Committee[6] by the Joint Councils of the Public Sector Service Delivery Council (PSSDC) and the Public Sector Chief Information Officer Council (PSCIOC) are important and admirable early steps in developing and securing Canada's digital economy. But more needs to be done and, while government continues to lead the way forward, it cannot accomplish this formidable task alone. The private sector must continue to get involved as the government provides the regulatory and economic climate for this to happen.

A tremendous opportunity for Canada

DIACC sees an opportunity to drive transformational change for businesses, governments and citizens across Canada. In the same way that our ancestors built a national railway that linked communities from across the country and created new markets, broad adoption of a modern, robust digital identification and authentication ecosystem will link us online and create new ways of interacting with each other and with others around the world.

In the same way that building the railway stimulated new engineering and led to spin off and ancillary business opportunities, the move toward digital authentication will create greater demand for skilled resources and new technologies. In the same way that the railway increased employment opportunities and enabled Canadians to participate in society on a more equal footing, digital identification will create a more level playing field across Canada.

[5] See: http://bit.ly/1Dgqeyd

[6] See: http://bit.ly/1yWRBCi

Board of Directors of the Digital Identification and Authentication Council of Canada

Dave Nikolejsin
Chair, DIACC
Deputy Minister, Province of British Columbia

Corinne Charette
Senior Assistant Deputy Minister, Industry Canada

Eros Spadotto
Deputy Chair, DIACC
Executive Vice-President, Technology Strategy, TELUS

David Nicholl
Corporate Chief Information and Information Technology Officer, Province of Ontario

Rizwan Khalfan
Senior Vice President - Digital Channels, TD Bank Group

John Jacobson
Deputy Minister, Technology, Innovation and Citizens' Services, Province of British. Columbia

Marlene Lenarduzzi
Vice-President North American Business Services, BMO Financial Group

Andre Lesage
Vice President AccèsD, Desjardins

Graeme Gordon
Vice President, Canada Post

Table of Contents

INTRODUCTION— LET'S BUILD A ROBUST DIGITAL ECOSYSTEM

As Canadians, we face a significant challenge in how we transact online. This challenge is causing massive waste and friction in the economy. It is leading to enormous fraud. And it is creating frustration and inconvenience for Canadians on a regular basis.

Canada, long recognized as a digital leader, risks falling behind in the emerging digital economy. A major reason for this reality is Canada's lack of a robust digital identification and authentication regime—a critical component of all digital activities.

Fortunately for Canada, the challenge is solvable.

In 2012, leaders from the public and private sectors in Canada gathered to create the Digital Identification and Authentication Council of Canada (DIACC).[7] The DIACC was formed to discover the best way forward for developing a robust, secure, scalable and privacy-enhancing digital identification and authentication ecosystem that would suit the needs of all stakeholders. Such a regime would touch on all aspects of commerce and information sharing. It would enable people to interact and transact online with confidence and minimum risk to their personal information. It would be at the core of transforming how we interact online and how we will acquire goods and services in the future.

In this report we propose ways in which such a modern digital identification and authentication ecosystem can create new economic opportunities for Canadian consumers and businesses, improve how services are delivered, decrease costs for businesses and governments and, ultimately, drive GDP growth.

Canadians are ready to live in a secure digital world

Canadians are increasingly comfortable in the digital world and have moved online with confidence. In 2014, nearly 87 percent were connected to the Internet.[8] However, Canadians have legitimate concerns about fraud, identity theft and system failures. According to the Canadian Anti-Fraud Centre nearly 15[9] percent more people reported identity theft in 2013 than in 2011.

In addition to identity theft, Canadians are constantly reminded of how the information they share online may not be adequately protected. In 2014 alone, Canadians were alarmed and in some cases deeply affected by such issues as the Heartbleed vulnerability and major breaches at retailers such as Target and Home Depot and government organizations such as Canada Revenue Agency and the National Research Council of Canada.

It is no wonder that Canadians are concerned that their online information is vulnerable and that their privacy is eroding. Recent headlines suggest hundreds of health record breaches. According to the Office of the Privacy Commissioner of Canada, 66 percent of Canadians perceive that they have lost privacy over the past few years and 71 percent believe that protecting personal information will be among the most important issues for Canada in the next 10 years.[10]

Canadians have a compelling interest in controlling what others can learn about them. Put simply, many Canadians seek to minimize external usage of their personal information. That said, Canadians are extremely high adopters of

[7] The establishment of DIACC was a recommendation of the Task Force for the Payments System Review.

[8] 2014 Canadian Internet Registration Authority (CIRA) Factbook: http://www.cira.ca/factbook/2014/index.html

[9] See: http://bit.ly/1EvmIHl

[10] Survey of Canadians on Privacy-related Issues. Office of the Privacy Commissioner of Canada. January 2013.

loyalty programs that trade in personal shopping behaviour data in exchange for shopping rewards. Recent studies suggest that Canadian consumers (carrying on average four loyalty cards in their wallets) opt into loyalty programs that are user-centric and deliver high value.[11]

Digital identity is defined by the Government of Canada as: "an identity developed in the online environment that can be accessed, used, stored, transferred or processed by means of electronic or computer devices or systems."[12]

Unlike traditional real-life identity, digital identities can range from a simple username/password unrelated to a person's specific attributes or may be tied to personally identifiable information from official credentials such as a passport or driver's license. Increasingly advanced biometrics such as fingerprinting, iris or retinal scans or cardiac signatures are forming a component of digital identities. Canadian startup Nymi is a leading example of the latter.

It becomes clear, therefore, that it is possible—indeed probable—that individuals will have more than one digital ID for their various online activities. Canadians will have separate online identities for interactions such as opening a bank account or joining an online dating site, each of which needs to be updated as the person ages, moves residence or undergoes some other status change. Unfortunately, Canadian citizens and businesses today have limited convenient choices for addressing their digital identity needs and are currently plagued by online maladies.

A common complaint is the challenge of maintaining passwords. Studies have shown that many people either reuse the same password repeatedly or choose to write their passwords down in a book that could be lost or stolen. What happens when one password is compromised? What happens when an Internet vulnerability like Heartbleed requires a reset of hundreds of your passwords? What happens when you share temporary access with a friend or family member? Why are the most common passwords "password", "123456" and "QWERTY123"?

A researcher from the University of Cambridge studied just how rampant the problem of password reuse might be, and his conclusion was very disturbing. He compared recently stolen login information for two different websites, rootkit.com and gawker.com. Between the two sets of data, he found an intersection of 456 legitimate email addresses, and the password reuse rate among those addresses was at least 31 percent. The figure could be as high as 43 percent—or 49 percent if you count the use of similar passwords, such as instances where the different characters are capitalized (Hello vs. hEllO) or a number is appended to the password (Hello vs. Hello1).[13]

Some organizations attempt to address these issues by forcing users to have longer or more unique credentials or even randomized strings. Without regular use or an association to help prompt a user's memory, these passwords are subject to another modern invention: the password reset.

The Government of Canada has addressed these issues. It has adopted a standard approach to credentials and has purposely separated them from identity information. The SecureKey Sign-

[11] "Talking Loyalty" Yahoo Canada, March 2015.

[12] See: http://bit.ly/1EmTHvq

[13] See: http://bit.ly/1DT1oYQ

In Partner Login for Government of Canada is an example of a program that works. SecureKey minimizes the need for users to remember multiple passwords by allowing users to sign in using a username and password from another reliable system—for example, a major bank. The service acts as an information filter to ensure that the government services do not know which sign-in partner is used, and that no sign-in partner knows which government service is being accessed.

The alternative solutions are not good enough for Canadians

Historically, Canadians have not been concerned with data minimization—that is, supplying only the data absolutely needed to effect a transaction. Likewise, the institutions with which we transact have not been focused on data minimization, often willing to collect as much information as they could about an individual "just in case" it could be valuable in the future. Modern liability concerns and fears of creating unjustifiably rich pots of personal data have changed this mentality. Unfortunately, our ID is slower to change. We often hand over driver's licenses to be allowed to buy alcohol, handing total strangers unnecessary data such as our full name, address, date of birth, height and even a scan of our signature. Why? Because we accept that it is the easiest way to prove that we have reached the age of majority. Each time we hand over our personal information we risk it being used for purposes that we cannot control.

Many Canadians use authentication services such as Google and Facebook to login to other online services. Most of us are guilty of not reading the terms and conditions, which means we do not understand or fully appreciate the data collection and sharing implications of our actions. While we have one less password to remember and we gain a convenient shopping experience, the suppliers of convenience are collecting information about our interests, our usage, what we say, to whom and our location 24/7. Often, we do not know who else this information is being shared with and for what purposes, and the experience is not designed to guide us or ensure that we make an informed decision. These are not user-centric experiences with privacy by design defaults. The impacts for Canadians are lower security and reduced privacy.

Impact on business

The world is turning to online services for transactions. Canada needs to do so in a manner that is easy for Canadians to use, yet preserves our confidence and trust in the overall ecosystem.

Remembering your corporate passwords is an expensive challenge. A study by Forrester Research estimates that the average help desk labour cost of a corporate password reset is approximately $70, with an average of 3.3 help desk calls per user per year. For a firm with 5,000 employees, this translates into annual costs of more than $1.1 million on employee password resets alone.[14]

Proving who you are online is a challenge. Know your customer (KYC), anti-money-laundering (AML) and terrorist financing (TF) regulations were created to monitor large-value financial transactions in a systematic manner. These regulations represent global expectations for our country and demonstrate that we will do our part to keep the world safe. Yet these regulations have created unexpected barriers and costs for many businesses that simply want to do business. Why does it take so long to close a real estate deal in Canada? Transactions are studied for possible involvement of proceeds of crime or terrorist financing. With digital ID and authentication, we could potentially decrease the screening time.

[14] See: http://bit.ly/1HO1gMW

Inconsistent regulations are a challenge. Regulations vary from province to province. For example, one can use an e-signature to purchase property in BC but not in Ontario. Regulations also vary from industry to industry. For example, one can use an e-signature to purchase property in BC but one cannot purchase and activate a cell phone online anywhere in Canada. Without a consistent approach to regulation, it is difficult for any solution to scale. Businesses are opting not to invest in online solutions and continue to rely on face-to-face transactions. In today's day and age, should a business be forced to scale their physical presence to scale their business presence?

Impact on governments

"Digital First." "Mobile First." These are the rallying cries of new champions of electronic service delivery. Municipal, provincial and federal governments in Canada all have plans to improve services and reduce costs by shifting to online channels. Canadians expect to reap the rewards of convenience and service improvement. We want the best service (high quality, error free, specialised knowledge), fastest, shortest turnaround times, and longest hours at the lowest cost.

Rural service delivery has always been a challenge in Canada due to our vast geography. We see this problem accelerating as more youth leave rural and remote parts of the country seeking education and employment—literally leaving an aging population behind "back home." Providing Canadians with comparable levels of service, regardless of geographic location, really calls for leveraging the power of the Internet.

The Government of Canada wants to move forward more aggressively in providing online access and online services to citizens and businesses, regardless of their location. To do so we need trusted identity and credentials that can be used online.

> In most of society's transactions, organizations are not interested in evidence to establish the identity of the person, but are instead interested in evidence to show something else. For example:
>
> - A merchant is interested in establishing that the customer is entitled to use the credit card presented to the merchant.
> - A bus driver is interested in knowing that the ticket (or "token") used to enter the bus is valid. The driver has no interest in knowing anything about the passenger, unless the passenger is using a ticket such as a student discount ticket, in which case the driver may want some proof of student status to confirm the passenger's right to use a student ticket. Even here, the bus driver does not need to know the identity of the person, merely that the person possesses the attribute of being a student.
>
> Where a business or government agency doesn't really need to know the individual's identity, but merely that the individual is authorized to do something (use a credit card) or entitled to receive something (a government benefit), individuals can protect their privacy by restricting the identifying information that they surrender about themselves. This limits the ability of others to monitor their activities and profile them.
>
> —Office of the Privacy Commissioner of Canada, 2008[15]

[15] See: http://bit.ly/1GsUGau

Building a model that works for Canada

New models are being developed. Over the past several years, the public sector has been diligently building a solid foundation of strategy, policy and standards. These efforts are beginning to coalesce into a model for Canada.

Starting in 2007, the Inter-Jurisdictional Identity Management and Authentication Task Force (IATF) published the Pan-Canadian Strategy for Identity Management and Authentication.[16] In 2010, the Identity Management Steering Committee (IMSC) published the Pan-Canadian Assurance Model and, in 2011, published Trusting Identities: Pan-Canadian Approach to Enabling better Services for Canadians.[17] In late 2014, the Federal Provincial and Territorial (FPT) Deputy Ministers' Table on Service Delivery Collaboration approved the Pan-Canadian Identity Validation Standard, which standardizes identity validation requests and responses between federal, provincial, territorial and municipal government organizations. This standard is an evolution of the National Routing System (NRS),[18] a multi-jurisdictional effort to improve the collection and validation of birth and death information from provincial vital-event registries. Canada's Digital Interchange is a multi-jurisdictional strategic initiative to develop a new capability of electronically confirming an individual's identity information securely and in near real-time.

Practical guidance has also been developed:

- The Office of the Privacy Commissioner has published guidelines on Authentication and Identification.
  http://bit.ly/1JyXE3n
- Industry Canada has published Canada's Principles for Electronic Authentication.
  http://bit.ly/1zlARVs
- Treasury Board Secretariat has published the Directive on Identity Management, the Standard on Identity and Credential Assurance, and related guidelines.
  http://bit.ly/1zlB4YU

Identity legislation is being enacted. In 2011, the Province of British Columbia amended the Freedom of Information and Protection of Privacy Act to include a designation of a provincial identity information services provider (PIISP) with authority to provide the specific services for the Province of British Columbia.

These foundational pieces are beginning to form a model for Canada but we still need to develop a model for a pan-Canadian digital identity ecosystem that will enable all players (public and private) to safely and securely use their digital identity online. In the absence of a collaborative effort, different sectors such as financial institutions, telcos and others would likely build or join industry-specific solutions to serve their respective constituencies. It seems obvious that many would prefer a collaborative approach to build trust and adopt a more general purpose, sector-independent, interoperable digital identity ecosystem.

Efforts to date have led to the emergence of a simple, compelling model called the Federated Authentication and Brokered Authorization Model. The model involves four main actors (See Figure on page 16):

1. **The individual**—The person seeking to provide proof of their identification to conduct a digital transaction or interaction

[16] See: http://bit.ly/1ySX7pk

[17] See: http://bit.ly/1JgByT7

[18] See: http://bit.ly/1DUyLr1

2. **The relying party**—An organization, individual or system that needs to access an authoritative party as authorized by the user (individual)
3. **The authoritative party**—An approved, recognized or trusted body that provides assurances (of credential or identity) to relying parties
4. **The core digital identification and authentication platform service**—A digital identity infrastructure service consisting of separate, bounded, discrete components for:
   - personal agents (whether mobile device based or Web-based)
   - authentication services
   - core registrar/identifier exchanger service

Canadian stakeholders are excited to address the opportunity before us and eager to dive into what more needs to be done. We require a made-in-Canada solution that can be part of the global solution to digital identification and authentication. We need to define our own solution for several compelling reasons:

1. **Canadian principles**
   Canadians use identity that is defined here and that reflects our unique perspective of privacy, trust, respect and accessibility. We seek to promote an ecosystem that enshrines our principles.
2. **Canadian business model**
   Business models designed here are more likely to favour and reflect the needs and interests of the Canadian economy and stakeholders. Cost and savings created by implementing and using digital identification will be realized here, by local businesses, rather than by foreign or international organizations. The solution should be designed to deliver maximum benefit and impact for us.
3. **Canadian regulatory model**
   The legislative and regulatory model that will govern this ecosystem will be Canadian and we should promote an ecosystem that ensures compliance with all regulators, including privacy commissioners, and removes jurisdictional conflict.
4. **Technical model and architecture**
   The technical infrastructure on which this ecosystem will operate needs to adhere to local standards and integrate with existing systems. There are substantial benefits to building solutions that integrate to and enhance current Canadian architectures.

What DIACC has accomplished

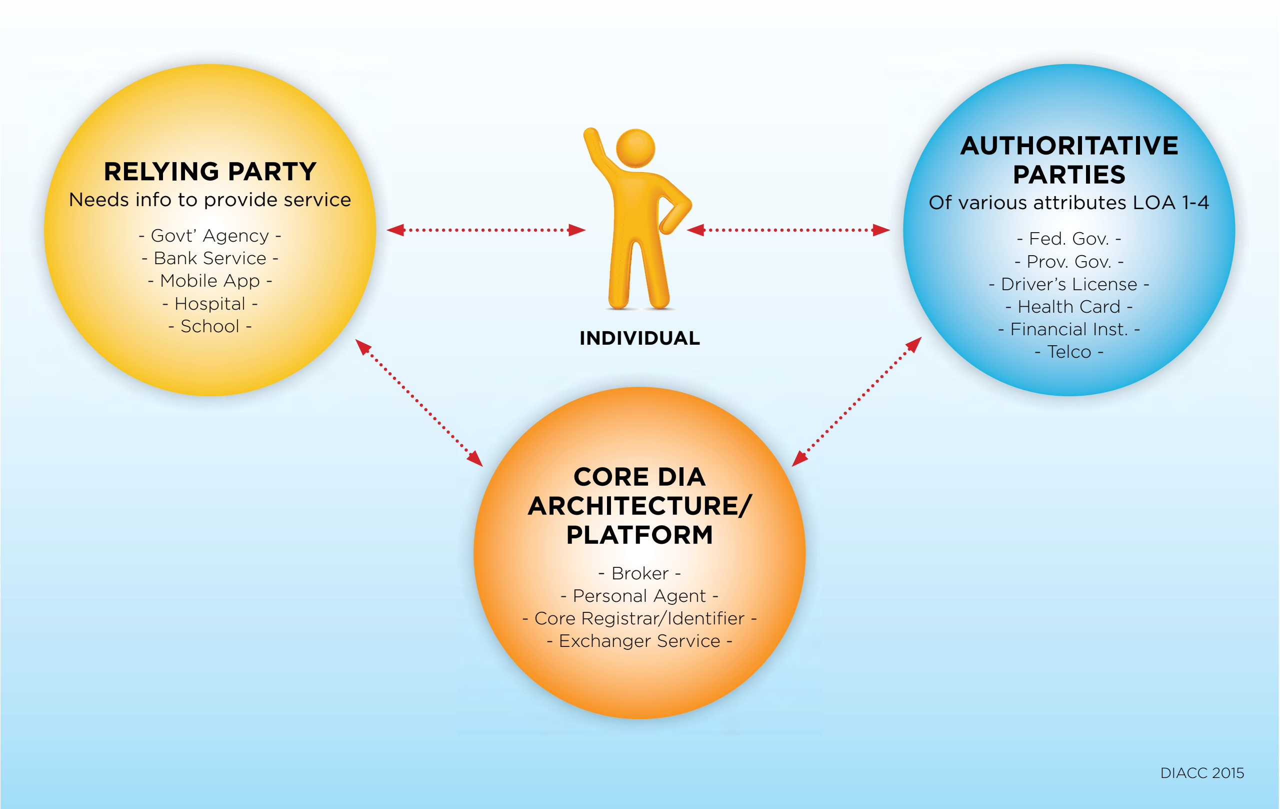
The Digital Identification and Authentication Council of Canada (DIACC) is the non-profit coalition of public and private sector leaders committed to promoting the development and adoption of a trusted Canadian ecosystem for digital identification and authentication that will enable Canadians' full and secure participation in the global digital economy.

Our mandate is to better understand what is needed in a pan-Canadian approach to digital ID and authentication, and to facilitate the development and adoption of interoperable policies, standards and systems.

DIACC's members and advisors include leaders from both the federal and provincial levels of government as well as representatives from small and large businesses and charities. DIACC has sought and received comment and guidance from privacy commissioners at the federal and provincial levels.

DIACC is aligned with the Government of Canada's Digital Canada 150 program. Digital Canada 150 is an ambitious program working to ensure that all Canadians have equal access, and are therefore able to take equal advantage of, the benefits a connected world can offer. The Government of Canada's Digital Canada 150

FEDERATED AUTHENTICATION AND BROKERED AUTHORIZATION MODEL



program also promises to strengthen the *Personal Information Protection and Electronic Documents Act* and is striving to provide Canadians with greater access to government services and research.

> "This unprecedented collaboration will provide Canadians with a framework to transact with ease and security when and where they want to while maintaining their desire to keep a degree of separation between information shared with the private and public sectors."
>
> —Rizwan Khalfan, SVP, Digital Channels, TD Bank Group.

DIACC is actively collaborating with two pan-Canadian Councils: the Public Sector Service Delivery Council (PSSDC) and the Public Sector Chief Information Officer Council (PSCIOC). Each council consists of senior officials representing the federal, provincial/territorial and municipal levels of government. The councils meet regularly in person and via teleconference, both separately and as the Joint Councils.[19]

Reporting to the Joint Councils is the Identity Management Sub-Committee (IMSC),[20] the mandate of which is to

- "represent the broader public sector perspective through the facilitation of consultation, dialogue and discussion among the jurisdictions,

[19] See: http://bit.ly/1FgIFsz

[20] See: http://bit.ly/1yWRBCi

- develop working papers, strategies, policy positions, and recommendations that can be used to provide a consistent pan-Canadian approach to address identity management issues extending beyond the public sector, including long-term identity management governance; and,

- promote the sharing and flow of information among jurisdictions, including the sharing of best practices, and discussion of issues. This includes the monitoring and reporting of progress on initiatives being carried out within the jurisdictions."

The IMSC also provides regular updates to the Federal-Provincial-Territorial Deputy Ministers' Table for Service Delivery Collaboration (FPT DM Table). DIACC, by working with these public sector bodies and bringing the viewpoints of our private sector members to them, hopes to build a digital ecosystem that serves the needs of all Canadians.

Over the last 10 months, DIACC has organized contributing members of the council into working groups focused on identifying and defining the requirements for the development and adoption of a pan-Canadian digital identification and authentication framework and ecosystem.

From April 2014 to February 2015 DIACC developed:

1. **The Federated Authentication and Brokered Authorization Model,** which is a proposed approach for Canada's digital identification ecosystem that considers the broad set of uses across different sectors, both public and private. Included with this recommendation is a roadmap of next steps we will need to take to realize such an ecosystem.
2. **A set of recommended enhancements** to existing regulations and legislation required to support the digital ID ecosystem.
3. **A proof of concept demonstration** of a differentiated experience of opening a bank account online at financial institutions without the benefit of an in-person, know-your-customer experience.
4. **Stakeholder consultation** providing key considerations for meeting positive user acceptance objectives.

A CANADIAN SOLUTION TO IDENTITY

Canada's economic future depends on developing a robust, secure, scalable and convenient ecosystem for digitally validating an individual's identity. We need a made-for-Canada solution that will reflect and incorporate Canadian principles, support Canadian business interests, support existing Canadian technical models and architectures, and support and demonstrate compliance with Canadian laws and regulations.

Any ecosystem that Canada adopts must be trustworthy and reliable, and place the individual in control of whether their personal or private information is shared, with whom and for what purpose. These elements are non-negotiable if Canadians are to adopt an ecosystem to the extent that it will flourish. Canadians expect their digital identification infrastructure to operate with transparency and openness, inviting them into the development process and ensuring their interests are represented throughout. This means that Canadians expect clear, meaningful and prominent notice about how, by whom and for what purpose their digital identification and information is being used.

This report identifies technical, business and regulatory models that support pan-Canadian expectations while creating a secure, scalable, privacy enhancing, cost effective and convenient ecosystem upon which Canadians can conduct a wide range of secure online transactions and interactions.

> "With a robust and effective digital ID and authentication framework, Canadians from coast to coast to coast will be able to engage with both the public and private sector digitally, in a manner that is safe, secure and efficient—be it to open a bank account or to register for government services."
>
> —David Nikolejsin, Deputy Minister at Government of British Columbia

The Digital Identification and Authentication Council of Canada proposes the Federated Authentication and Brokered Authorization Model ecosystem as a solution. The model is built on the seven universal requirements of a digital ecosystem as well as four specifically Canadian requirements.

The seven universal requirements of a digital ecosystem

1. Robust, secure, scalable
2. Privacy protecting/privacy-enhancing
3. Inclusive and transparent
4. Meets broad stakeholder needs
5. Data minimization
6. Knowledge and consent
7. Convenient

1. Robust, secure, scalable

Canada's digital identity ecosystem must be robust enough to ensure it is secure, available and accessible 24/7, 365 days a year. This will require building in redundancy and disaster recovery tools strong enough to withstand any outage.

The infrastructure for such an ecosystem must be built in such a way that it can leverage the latest advances in security. Protecting how information is used is of paramount importance and the infrastructure design must take into account best practices for securing information, such as encryption and second-factor authentication. The goal of cybersecurity is to protect data both in transit and at rest. The infrastructure must rely on a foundation of access control, awareness training, audit and accountability, risk assessment, penetration testing and vulnerability management. Continual security assessments must be built into ongoing operations.

The proposed solution must be scalable to meet not only today's requirements but also tomorrow's. One reason we chose a broker model as opposed to a direct link between relying parties and authoritative parties was to ensure that the solution would be scalable. While direct relying party to authoritative party connections are acceptable and could work within the model, one can quickly see the chaos and bottlenecks that could occur once you have millions of relying parties trying to directly connect to and access thousands of authoritative parties and vice versa. The model we propose is scalable and allows for the use of multiple technologies, as the broker/personal agent/proxy/delegated authority can connect to various technologies (allowing for change over time). A direct model, by contrast, would require a single technology platform, which could quickly become obsolete and would be a target for hackers.

The ecosystem must also scale as needed, that is, it must be flexible enough to allow participants to enter at their own speed. Some provinces are further along than others in issuing identity cards that can be accessed digitally. Some organizations are ready to accept digital identities; for others the investment will have to wait. It will also take time for some users to adopt this method. The ecosystem must be designed in such a way that governments, businesses and users are able to join when they are ready.

2. Privacy-protecting by design/ privacy-enhancing

In the digital world, privacy is about controlling who has access to your data and how they are permitted to use the data.

When DIACC examined privacy issues, we focused on how privacy can be incorporated into the foundation of all digital transactions and interactions. While every individual must sacrifice a degree of anonymity to transact and interact online, the issue becomes: how much anonymity must I sacrificed and how much information must I provide. Furthermore, we must consider how the receiver of our personal information (e.g., private company, government, individual) is permitted to use it.

2-factor authentication:

Depending on the level of security (assurance) that a transaction requires, 2-factor authentication may be a requirement for security, privacy and safety of information. With 2-factor authentication, a person must have a PIN number or password to enable their ID card, phone, wrist-band, etc. Using 2-factor authentication, if you misplace or have your card or device stolen, it is merely an inconvenience to replace—as opposed to an immediate worry that someone might steal your identity for devices that do not rely on PIN and passwords. Most very secure transactions will be satisfied by 2 factor authentication, but for extremely secure transactions (Assurance Level 4) biometrics (for example unlocking your mobile advice with your fingerprint) will also become a more mainstream option.

For example, if you are trying to purchase alcohol you must show photo identification to prove you are the age of majority. Most people use their driver's license for this purpose; however, a driver's license provides a great deal more information than just your age. At minimum, it also provides your name, your precise date of birth, your address and, potentially, your organ donor status. To purchase alcohol, however, all you need to do is prove that you are the age of majority; you do not need to indicate precisely how old you are. One can easily imagine an ecosystem in which consumers never hand over their ID, but simply tap it against a merchant terminal or other device. If the consumer resembles a photo displayed on the terminal, and that identity is of the age of majority, a green check mark appears. In this scenario, the merchant has fulfilled a regulatory need and the consumer has retained control of their information.

This is the approach that we took when looking at privacy in the digital age.

As a starting point, we used the Privacy by Design principles developed by Dr. Ann Cavoukian during her time as Privacy Commissioner of Ontario to examine privacy in the digital age:

1. Proactive not reactive; preventative not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality—positive-sum, not zero-sum
5. End-to-end security—full lifecycle protection
6. Visibility and transparency—keep it open
7. Respect for user privacy—keep it user-centric

To read more about Dr. Cavoukian's Privacy by Design principles, please see: [www.Privacybydesign.ca]

A critical component of privacy is for those using the system to be informed of what they are sharing, to whom and for what purpose, as well as providing consent for that information to be shared and used.

An individual can give informed consent only when they have a clear understanding of the facts, implications and potential consequences of an action. One aspect of giving informed consent is for the individual to maintain control over their personal information throughout the entire process of submitting ID as well as maintain a clear understanding of how that information will be used. The Authorizing Broker Model holds that when an individual or their agent initiates a transaction or registration, they must be provided with a general description of the service and how it operates. This includes what information, if any, may be released by default to the ID requesting relying party. If the individual indicates intent to use the broker service to gain access to services or applications, the authoritative party must make available to the individual a description of what additional information, if any, may be released to such applications. The individual must indicate consent to these provisions before the transaction can be completed. The authoritative parties should provide a mechanism for individuals, or their agents, to deny release of individual attributes to applications.

In addition, if individuals are allowed to establish a continuing approval or denial for release of certain attributes—for example, to avoid being asked anew each time they make a transaction—there must be some mechanism by which individuals can alter or withdraw any of those established preferences.

3. Inclusive and open

Canadians need to trust that any proposed models will protect their private information. They need to believe that newly proposed models are an improvement over the current way of doing business. They also need to understand that they will have greater control over how much of their personal information they are sharing, who will use that information, and how it will be used.

As we developed the Federated Authentication and Brokered Authorization Model (see the Technical Model and Architecture for details), DIACC spoke with Canadians to gauge their views, concerns and expectations. Rather than asking broad questions, we sought comments and views from a variety of consumer and user groups across Canada about a specific activity that required digital identity to be realized: the ability to open a bank account online without a prior know-your-customer (KYC) experience. Current regulations require an in-person visit to a branch to open a bank account for the first time.

There are a number of online banks that claim to let you open a bank account online but only if you already have an existing account with another financial institution (this other account is what they use as your digital identification). In our proposed scenario, Canadians could login via the Web or their mobile device and within minutes open a new account with a financial institution.

Nine organizations, including the Consumers Council of Canada, the Public Interest Advocacy Centre and the First Nations bank of Canada offered us their expertise in consumer affairs or financial services, and DIACC conducted telephone interviews with them between May and July 2014 to hear their opinions about the Federated Authentication and Brokered Authorization Model. Our interviewees told us that consumers would benefit from greater convenience when banking online (especially those living in remote communities) and a wider choice of banking options. The banks themselves would benefit by attracting new customers, providing more products and services and increasing operational efficiency.

The concerns our interviewees raised were mainly on the subject of privacy, security and technical considerations. We deal with these issues in Appendix E—Ecosystem, privacy and user experience requirements met by the Federated Authentication and Brokered Authorization Model.

4. Meets broad stakeholder needs

The digital identity ecosystem must be affordable, standardized and of benefit to all Canadians. It must be flexible enough to adapt to new technologies and affordable enough for all Canadians to use. The ecosystem must be beneficial for banks, telcos and technology providers by providing new sources of revenue and service offerings. Federal, provincial and municipal governments must be able to better service their constituents while keeping costs to a minimum. Consumers must benefit from having equal access to goods and services regardless of geographic location and be able to save time by accessing such documents as vaccination records online rather than going to a doctor's office, or signing a waiver for a child's summer camp while away on a trip. The ecosystem must also be accessible to all Canadians, regardless of different abilities.

5. Data minimization

Users should be required to share only the minimum amount of information for completing an interaction or transaction. Using the alcohol purchase scenario once more, the only information needed is confirmation that the individual making the purchase is the age of majority. The party requesting confirmation of the buyer's age of majority status would not be entitled to any other information. Data minimization gives Canadians maximum control over the privacy of their personal information, and data minimization is a legal requirement under Canadian provincial and federal privacy law.

Encrypted or coded information could be used to further secure data in some situations. This would minimize the risk of data being used for purposes other than the original one. Another benefit of encrypted and coded information is that it ensures the ecosystem does not provide the relying party or the authenticating party with common identifiers that could be used to correlate user activity. For example, there is no reason to keep a record that age verification is being sought so that someone can buy alcohol—just that age verification is being sought. There is also no need to keep a record of how often age verification is sought.

Where possible and appropriate, anonymous transactions should be allowed and supported. This is critical if Canada is to embrace an ecosystem in which people engage in activities such as e-voting.

The principle of "data minimization" means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it.

—European Data Protection Supervisor
http://bit.ly/1asqX7L

6. Transparent in governance and operation

The topics of identity, authentication and privacy are as sensitive as they are important.

Few subjects have the potential to polarize a community in the way that privacy, control of our identity, and ownership of personal data can. Discussion tends towards the emotional as our opinions are rooted, by nature, in very personal beliefs, fears, and values.

For these reasons, it is important that we establish this new ecosystem such that it is transparent in both governance and operation. Canadians must be able to see how policy and decisions regarding their identities, privacy and data are made, and they must be able to observe how the infrastructure works to secure their transactions. Anything less than full transparency will foster mistrust and fear, or perhaps worse: apathy and disengagement.

Canada and Canadians have proven to be leaders when it comes to the principles governing digital identity. Historic leadership by Canadians like Kim Cameron (7 Laws of Identity), Dr. Ann Cavoukian (Privacy By Design) and others continues today with the works of dozens of leaders intent on enshrining key values in our digital identity systems. We must empower our Privacy Commissioners at all levels of government, Privacy Officers, Ombudspersons, and principled leaders across the country as they continue to work tirelessly to help Canadians navigate an emerging digital experience.

While Canada is known as a bastion of free speech, tolerance, and mutual respect, we must also work to protect our reputation as a digitally enabled country that enshrines key values as it moves forward. To gain the benefits of digital transactions - such as speed, convenience, and economies of scale - we do not need to sacrifice critical values like privacy, accountability and transparency.

7. Convenient

The ecosystem must be easy for users to access and interact with. Remembering dozens of passwords or carrying 15 different cards will not be acceptable. Users need the ability to validate their identification quickly and easily using one or multiple devices. Downtime must be kept to a bare minimum. It is sometimes surprising to think how often we need to identify ourselves. Consider going to the doctor and providing your health card, or going to the box office to pick up pre-ordered concert tickets. In both these cases the only way to ensure access is to have ready access to a specific identifier. In one case it is your health card; in another it is the credit card you used to purchase the tickets. In both cases the user experience will be negative (missed appointment, missed concert) unless you can easily access the specific form of identity required.

In the event a user forgets their password (or other identifier) or loses their identification (or device upon which it is stored) they must also be able to quickly and easily re-engage with the ecosystem. The ecosystem must be secure enough to prevent fraud but convenient enough to allow for rapid re-entry.

Four additional Canadian requirements of a digital ecosystem

1. Built on open, standards-based protocols
2. Interoperable with international standards
3. Cost effective and open to competitive market forces
4. Able to be independently assessed, audited and subject to enforcement

1. Built on open, standards-based protocols

Adopting open, standards-based protocols for Canada's digital ecosystem will help protect against obsolescence, ensure interoperability and foster a dynamic environment with multiple suppliers, etc.

Building Canada's digital ecosystem on open, standard-based protocols will also ensure that the country is not locked in to any one specific technology (or supplier) that might become obsolete. The dangers of governments and companies locking themselves into closed ecosystems are clear and the risk of sub-par or time consuming rebuilds of the entire system must be mitigated.

Using open standards will allow different technologies to communicate and interoperate with each other. This is essential in a federated model such as Canada as it will allow the federal, provincial and territorial governments and the private sector to adopt solutions that best meet their specific needs while allowing them to interact and exchange information.

2. Interoperable with international standards

Interoperability and the emergence of global standards are the foundations of todays connected world. Much like standardized railway gauges allow for travel and the transfer of goods across countries, and the standardization of cargo container sizes reduces shipping costs interoperability and standards allow the world to communicate and help to lower costs while increasing innovation. For Canada to thrive in a global economy we will need to ensure that our digital identity ecosystem is able to interact and exchange information with systems around the world. Canada should be not only a signatory to international standards but at the forefront of developing them.

3. Cost effective and open to competitive market forces

As a foundational component of the digital ID ecosystem it is essential that the ecosystem is developed in a manner that respects budgetary constraints both today and in the future. Private sector enterprises rightly expect to make a profit from their activities. Ensuring the ecosystem is open to many competitors, representing multiple business sectors, each playing different roles will lead to decreased costs for consumers and increased innovation throughout the ecosystem.

4. Able to be independently assessed, audited and subject to enforcement

For Canadians to truly accept and trust a digital identity ecosystem, various controls must be put in place. Independent third parties should ensure that the members of the ecosystem are adhering to the accepted rules and regulations. Audits should be publicly available and organizations failing to measure up to their obligations should be sanctioned accordingly.

THE ECONOMIC JUSTIFICATION

Internet-based economic activity is expected to reach $4.2 trillion in the G-20 nations by 2016 or more than 5 percent of GDP. The digital economy—which can be defined as economic value derived via the Internet—is growing at more than 10 percent per year, significantly faster than the economy as a whole. The Canadian Internet Regulating Authority (CIRA) says that the digital economy currently accounts for 3 percent of Canada's GDP ($49 billion per year).

A robust, secure, scalable, privacy enhancing digital identity ecosystem that enables Canadians to do business more swiftly and easily will increase Canada's GDP. It will provide businesses with an opportunity to reduce costs by being more efficient and increase profits by offering Canadians more services. Consider the following realities.

The cost of maintaining the status quo

Asking customers to identify themselves by answering personal questions is an irritant. It can be time consuming and customers often cannot remember the answers to their own authentication questions. Furthermore, this process can add significant operations costs. For financial and insurance institutions a verbal identity authentication can take several minutes. We estimate that the financial and insurance sector is spending between $50 and $80 million a year on verbal authentication alone!

Extrapolating these costs across other business sectors such as Internet service providers, cable companies, telephone companies and retailers, verbal identity authentication costs in Canada balloon to well over $100 million annually. This impressive number does not include the cost of the time spent by customers identifying themselves, the frustration at having to identify yourself multiple times or trying to remember which favorite pet you selected as the answer to your secret question. Nor does this number consider the opportunity costs of customers disengaging and either taking their business elsewhere or not conducting the transaction at all due to the complexities.

Canada is at a crossroads. Where once we were leaders in the digital economy we have started to fall behind. If Canada does not act now we run the risk of losing our competitive edge. We also risk ceding control of our identities to foreign companies that may not share our pan-Canadian values of privacy and control over personal information. Maintaining the status quo means accepting:

- an inefficient user experience (individuals will be forced to continue to create, manage and use multiple accounts)
- the inability to participate in an increasingly digital world because we are compelled, either through regulation or lack of infrastructure, to use non-digital methods
- a heightened risk of fraud and identity theft (by falling behind other nations on security, Canada may become an easy target for intruders)
- the erosion of our competitive edge and loss of our valuable talent ("brain drain")
- a loss of entrepreneurs and investment that may end up fueling businesses in other countries

Digital identification has benefits for all Canadians

Canadians are enthusiastically adopting digital technologies and services to improve the way they work and enhance their lifestyle. The rapid adoption of mobile devices, mobile apps and cloud-based services have the unprecedented capability of transforming entire industry sectors. Online transactions and interactions are now ubiquitous in the daily lives of Canadians. Whether it's paying bills, ordering theatre tickets or taking university courses online, Canadians are already using digital identities. Now imagine a world where Canadians can go online to vote, access their medical records, open a bank account and sign a waiver for their children's hockey camp. The introduction of a robust, secure, scalable and privacy enhancing digital identification ecosystem will decrease costs for governments, consumers and business while improving service delivery and driving GDP growth. Below are some of the immediate and tangible benefits that will become available across a number of sectors after the adoption of digital identification.

> "Consumers are drawn to the convenience of new ways of paying for their purchases, whether online or in a place of business. To make sure consumers are safe in the face of change, innovation and emerging risk factors, it will be necessary to monitor and improve both old and new payment systems. Consumers want transaction systems to be secure and private."
>
> —Don Mercer, Vice President, Consumers Council of Canada

Financial services sector

We have already discussed how the annual verbal authentication costs in this sector amount to more than $50 million a year. With a robust ID ecosystem, the financial sector could realize the following savings:

- Process automation allowing customers to self-serve via the Web or a mobile device could reduce in-branch operating costs to about 5 percent of the current cost.
- Electronic invoices and payments combined with a reduction in the use of cheques could lead to $7 to $8 billion in direct annual savings.[21]

In addition to savings, the financial sector could increase revenues in the following ways:

- Reach customers anywhere in Canada (and potentially worldwide) as there is no longer a dependency on a bricks and mortar presence
- Offer mobile wallets, which provide consumers with convenience and provide financial institutions with valuable insight on consumer preferences and behaviours based upon the data collected from purchases (this data could then be monetized in a variety of ways)
- Incorporate user health or auto data when underwriting insurance policies so they can offer additional services

Telecom sector

The benefits for the telecom sector include:

- Ability to reach customers anywhere in Canada
- Reduction of the need for a bricks and mortar presence
- Reduced operating costs through process automation and decreased need for verbal authentication
- New business opportunities beyond being simply a conduit for communication, with the opportunity to monetize services such as mobile wallets

Retail sector

The benefits for the retail sector include:

- Growth in overall customers and revenue by transcending the limitations of physical stores to reach anywhere in Canada (and potentially worldwide)
- Opportunity to capture lost sales currently happening outside of Canada

[21] Digital Identities, Challenges and Opportunities, Report for Industry Canada February 2015, PwC

- Replacement of costly call centre operations with Web and mobile interfaces
- Ability to offer and introduce new products based on improved consumer data (subject to consumer opt-in)
- Ability to offer more personalized experience based on demographics, location, behavioural and preference data (subject to consumer opt-in)

High tech sector

The benefits for the high tech sector include:

- Job creation through demand for innovative technology solutions around identity management
- Increased confidence for companies hiring professionals born outside Canada, as employers will be able to easily validate Citizenship and Immigration Canada documents

Public sector

The public sector is an essential participant in the digital identity ecosystem as the originator of identity information, keeping vital statistics records at the provincial and territorial level and immigration records at the federal level. The public sector will also benefit greatly from a digital identity ecosystem. Consider:

- Secure, convenient, privacy enhancing, cost effective digital identification will enable federal, provincial, territorial and municipal governments to provide a consistent user experience to all constituents across multiple departments, systems, domains and jurisdictions.
- The government will be able to meet a key goal of Digital Canada 150 to allow greater data accessibility and provide authorized Canadians with access to scientific data funded by government.
- The government will be able to provide the same level of service to citizens and constituents regardless of geographic location.
- A robust digital identity ecosystem could reduce identity fraud, lessening instances of healthcare system abuse and abuse of entitlement programs.
- At present, government-issued identity cards such as driver's licences are used repeatedly to conduct transactions. What if the government could recover some of its costs by charging a nominal fee to access its identity databases if citizens so desired?

The intangible benefit of digital identity is the removal of fundamental friction points to unlock value, leading to growth of services, products and technologies, and transformative societal change.

These examples of cost reduction and monetization opportunities are just a few of the tangible benefits of digital identification across a few sectors. Much like a railway, the benefits of digital identification must be available to all Canadians.

THE REGULATORY MODEL

A great impediment to the adoption of a robust digital ID regime is the large number of obsolete regulations across the country that were never intended to govern how transactions are conducted, and therefore how we prove we are who we say we are today. Canada needs uniform and consistent regulations in the realm of digital ID in the same way we required standard railway track size when we built our great railroads. A holistic solution based on Canadian principles, a Canadian business model and a shared technical model and architecture is the only reasonable way forward if all provinces and regions are to understand and operate by the same rules.

> "Many northern residents live far from a bank branch. If regulations permitted remote identification and authentication, we could offer more convenient options and customers would have more choice."
>
> —Greig Cooper, VP Operations, First Nations Bank of Canada

As our society transitions to the digital world, in-person and paper-based processes, once the preferred method of service delivery, are now being replaced by digital alternatives.

This trend toward digital alternatives is transforming how we present ourselves in person and online. Canadian documents used for the purposes of identification and eligibility, such as the e-passport and the BC Services Card, are being modernized. These modernized documents, while preserving the traditional in-person and document-based presentation methods, represent the next step toward digital alternatives and can provide significant advantages over traditional identity documents (e.g., driver's licence, birth certificate, etc.) including:

- More robust authentication techniques where the document can be electronically authenticated by means of a secure reader (key to combating document and identity fraud)
- The elimination of expensive and error-prone paper-based evidence collection processes (e.g., photocopying a document and placing in a physical file)
- Ability to integrate multiple reliable sources of information to provide a more robust validation of the individual based on a preponderance of information versus the one or two methods that exist today

These physical cards, embedded with electronic capabilities, provide secure means for individuals to electronically authenticate themselves. As society moves away from the concept of physical presence and documents as a basis for transacting, regulations should follow. While modern identity documents and capabilities can enhance existing physical presentation and document authentication processes, these will eventually be replaced by digital equivalents. Thus, regulators need to contemplate a digital world that is equally or more secure than what exists today. Regulations must go beyond the physical realm and not lock everyone to the old ways of doing things.

Some of these digital equivalents include the ability to:

- Electronically collect and validate identity information versus the more difficult (and less reliable) visual document authentication and reducing errors due to manual transcription of data
- Use technologically secure methods to ensure that the individual is the legitimate owner (e.g., use of a PIN)
- Preserve privacy by collecting only the information that is required to meet regulatory requirements rather than providing too much personal information

For regulatory change, governments must lead the charge. For example, changes in financial regulations can ensure uniformity, and allow for secure digital equivalents that can underpin the fully modern payments system and digital identity ecosystem of the future.

Our recommendation: Targeted regulatory changes

There are many examples of regulatory changes required. For example, section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*[22] does not provide for electronic methodologies to ascertain identity. This has broad impact across many types of transactions—for example, attempting to open a bank account or cell phone account or virtually any other legal document generally relies on "wet signatures".

With these considerations in mind, we propose that section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* be amended. The regulations must allow for the option of a fully electronic (i.e., digital) method to ascertain identity provided that the electronic method is sufficient in strength to meet key identification requirements. We propose that this additional method be called "electronic confirmation of identity." Here is how it could work.

Electronic confirmation of identity (digital identification)

This method of ascertaining a person's identity consists of two parts:

- Electronically confirming the accuracy of a person's identity information using an accredited, authoritative source
- Ensuring that the identity information being confirmed relates to the person making the claim

These two parts relate to two key objectives that must be met when ascertaining identity:

1. **Accuracy of identity information**—Identity information about an individual must be accurate, complete and up to date. Accuracy ensures that the identity information represents what is true about the individual and that the individual truly exists (i.e., not a fictional or synthetic identity). Confirming the accuracy of information is also referred to as "identity validation" and may be provided by an authoritative party, such as a vital statistics agency.
2. **Linkage of identity information to the individual**—Identity information, once confirmed as accurate, must relate to the individual making the claim. Linkage ensures that identity information is not being fraudulently used by another individual. Ensuring the linkage of information is also referred to as "identity verification." A variety of techniques may be employed to ensure that an individual is claiming their own identity information and not that of another individual. Techniques include asking for shared secrets that only the individual knows, biometric comparison (facial recognition) and requesting the presentation of a trusted credential (electronic or physical) that was previously issued to the individual. Different techniques can also be combined to reduce the risk of fraud.

When both objectives are met, they can provide a high level of assurance—a legal digital equivalent—that an individual is who they say they are. These electronic methods can be better than traditional, in-person, document-based processes and provide the necessary certainty to carry out high-value transactions.

[22] See: http://bit.ly/1EvnILB

Electronic signatures

In addition to being able to conduct transactions when not physically present, Canadians need clarity and confidence about what constitutes a legal digital or electronic signature. Digital or electronic signatures are often considered to be a solution to digital identities. In reality, they are just one part of a person's digital identity—much like a signature on a driver's licence or on the back of a credit card is one component of authenticating who the holder of that document is. The digital world allows for multiple types of digital or electronic signatures. The decision to use one type of signature over another must be assessed by the party accepting it against many factors including risk, potential for fraud, accepted practice and cost.

The purpose of having a signature on a document, whether written or electronic, is to ensure the integrity and unaltered representation of a given transaction. A signature identifies parties who have entered into an agreement, confirms that they understood and agreed to the transaction—neither can claim ignorance once they have committed a signature—and provides a public record of the transaction. A signature also provides a record of the state of the document at the time the signature was made. In other words, the document cannot be altered following the addition of signatures.

Current situation for electronic signatures

As of January 1, 2015, pursuant to the federal *Canada Evidence Act*, *Personal Information Protection and Electronic Documents Act*[23] (PIPEDA) and *Secure Electronic Signature Regulations*,[24] a secure electronic signature is defined as being:

- unique to the person
- under the sole control of the person
- used to identify the person
- linked with the electronic document in such a way that it can be used to determine if the document has been changed since the signature was attached
- based on Public Key Infrastructure (PKI) technology

We consider these federal criteria to be highly prescriptive. Although we agree that they provide a high level of assurance, they may create unnecessary technical barriers and costs.

Provincial standards

In addition to federal rules on e-signatures, each province has its own set of standards and regulations. These vary province to province and in some cases from industry to industry. In Ontario, for example, you can sign certain contracts digitally but those dealing with agreements of purchase and sale of land are expressly forbidden under the *Electronic Commerce Act, 2000* (ECA).[25] In British Columbia, e-signatures are acceptable for the purchase and sale of land. This means, however, that you may not be able to sign to purchase property in Victoria from your office in Ottawa. At the very least, this leads to confusion within the marketplace. At worst it stifles commerce and potentially puts people afoul of the law or negates contracts signed in good faith.

Common rules for using electronic signatures

Canada needs a single set of rules governing what is an acceptable e-signature. We propose a legal requirement that a document may be signed using an electronic signature only if the signature used:

- is reliable for the purpose of identifying the person who signs an electronic document using an electronic signature
- is under the sole control of the person when signing the electronic document
- can be linked with the electronic document in such a way that it can be used to determine if the electronic document has not been changed since the signature was attached
- meets security requirements as prescribed by applicable agreements, legislation or regulation

[23] See: http://bit.ly/1Hu2oFe

[24] See: http://bit.ly/1ENB322

[25] See: http://bit.ly/1zbqy60

THE TECHNICAL MODEL AND ARCHITECTURE

Canada needs to develop a technical model for the nation's digital ID ecosystem that is positioned to meet an extraordinarily wide set of potential uses. DIACC members worked iteratively over several months to identify a technical model that holds the promise for all potential uses, conforms to and reinforces the seven principles, supports our business and economic needs, adheres to regulatory requirements and minimizes the cost of implementation by working with our existing infrastructure. It was a tall order.

The essential criteria

To determine their suitability we reviewed and assessed potential technical models, taking into consideration the criteria essential to any emerging digital ID ecosystem. The desired technical solution had to adhere to the following:

The seven universal requirements of a digital ecosystem:

1. Robust, secure, scalable
2. Privacy-protecting by design /privacy-enhancing
3. Inclusive and open
4. Meets broad stakeholder needs
5. Built to minimize data transfer
6. Transparent in governance and operation
7. Convenient

Four additional Canadian requirements of a digital ecosystem:

1. Built on open, standards-based protocols
2. Interoperable with international standards
3. Cost effective and open to competitive market forces
4. Able to be independently assessed, audited and subject to enforcement

DIACC also addressed the concerns that our stakeholders raised during a series of interviews in the following manner:

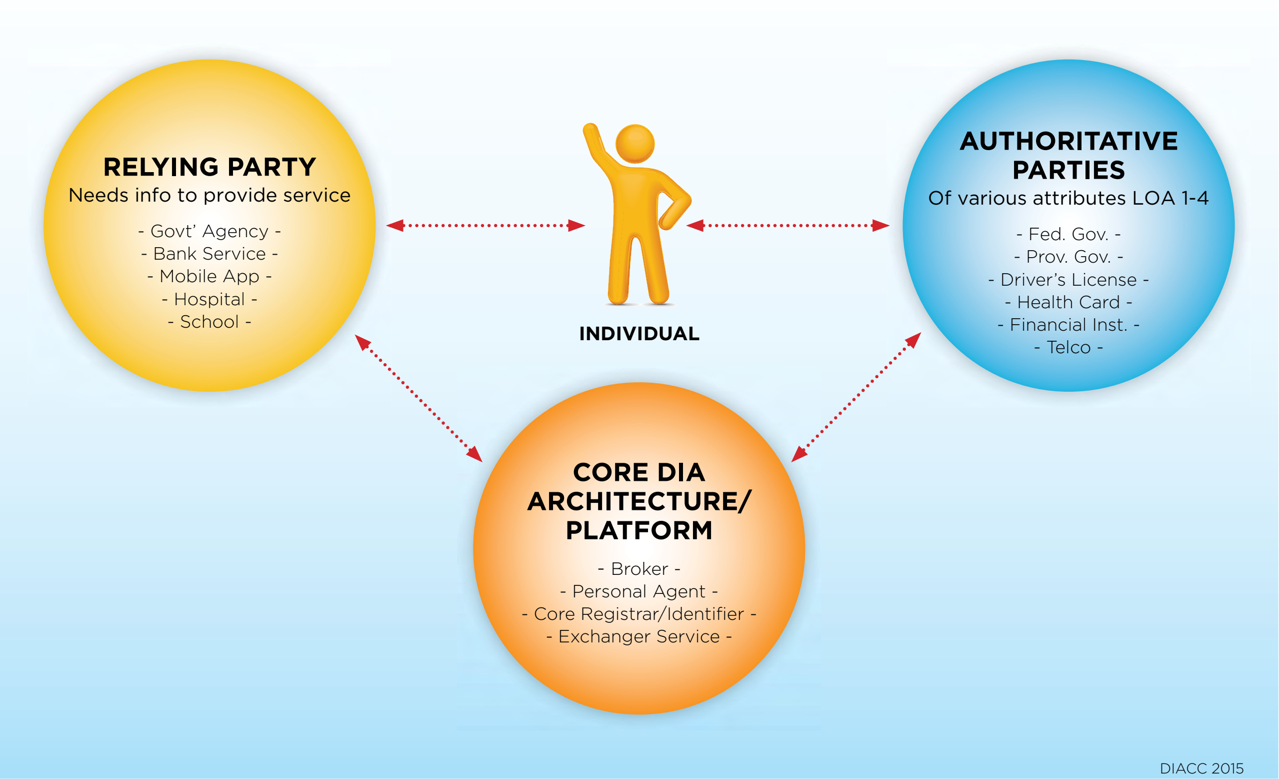
- The model takes into account a broad range of security and privacy considerations, including the issues and concerns raised in the interviews.
- We identified the regulatory and legislative changes required to ensure compliance with laws and regulations and we made recommendations to reflect advances in identity management technology.
- We consulted openly and transparently with various privacy commissioners to ensure the proposed solution adheres to and, in some cases, strengthens Canadian privacy laws and the desires of the Canadian people.

The Federated Authentication and Brokered Authorization Model

The Federated Authentication and Brokered Authorization Model supports the key criteria and considerations and known requirements for user experience, privacy, security and the technical platform. It also addresses the non-regulatory concerns raised during stakeholders interviews. The figure on the next page llustrates the Authorising Broker Model at a high level.

> Canada needs to develop a technical model for the nation's digital ID ecosystem that is positioned to meet an extraordinarily wide set of potential uses.

FEDERATED AUTHENTICATION AND BROKERED AUTHORIZATION MODEL



RELYING PARTY
Needs info to provide service
- Govt' Agency -
- Bank Service -
- Mobile App -
- Hospital -
- School -

INDIVIDUAL

AUTHORITATIVE PARTIES
Of various attributes LOA 1-4
- Fed. Gov. -
- Prov. Gov. -
- Driver's License -
- Health Card -
- Financial Inst. -
- Telco -

CORE DIA ARCHITECTURE/ PLATFORM
- Broker -
- Personal Agent -
- Core Registrar/Identifier -
- Exchanger Service -

DIACC 2015

Explained in simple terms, the Federated Authentication and Brokered Authorization Model involves four main actors:

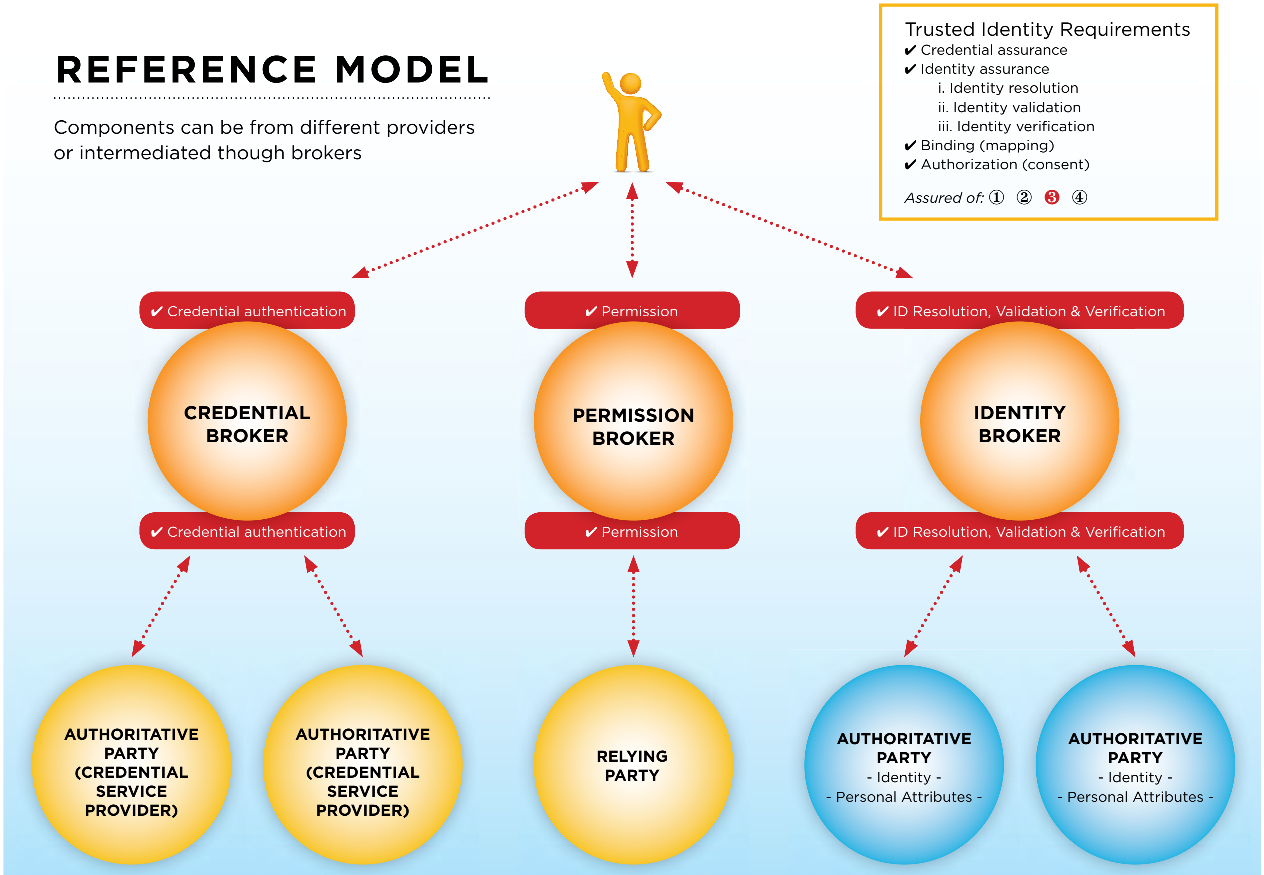
1. **The individual**—The person seeking to provide proof of their identification to conduct a digital transaction or interaction
2. **The relying party**—An organization, individual or system that needs to access an authoritative party as authorized by the user (individual)
3. **The authoritative party**—An approved, recognized or trusted body that provides assurances (of credential or identity) to relying parties
4. **The core digital identification and authentication platform service**—A digital identity infrastructure service consisting of separate, bounded, discrete components for:
   - personal agents (whether mobile device based or Web-based)
   - authentication services
   - core registrar/identifier exchanger service

Benefits of the Federated Authentication and Brokered Authorization Model

The Federated Authentication and Brokered Authorization Model meets all the criteria and considerations listed above and will provide Canadians with a secure, scalable, privacy enhancing, cost effective and convenient ecosystem. The Federated Authentication and Brokered Authorization Model is prescriptive enough to provide guidance and a strong level of assurance while remaining flexible enough to incorporate the introduction of new technologies or technical standards. Please see Appendix E to read about the specific ecosystem, privacy and user experience requirements that the model meets.

Model assumptions

Model assumptions were developed based on a review of different reference models. The following assumptions and the figure above


REFERENCE MODEL
Components can be from different providers or intermediated though brokers
Trusted Identity Requirements
✔ Credential assurance
✔ Identity assurance
i. Identity resolution
ii. Identity validation
iii. Identity verification
✔ Binding (mapping)
✔ Authorization (consent)
Assured of: ① ② ❸ ④
✔ Credential authentication
CREDENTIAL BROKER
✔ Credential authentication
✔ Permission
PERMISSION BROKER
✔ Permission
✔ ID Resolution, Validation & Verification
IDENTITY BROKER
✔ ID Resolution, Validation & Verification
AUTHORITATIVE PARTY (CREDENTIAL SERVICE PROVIDER)
AUTHORITATIVE PARTY (CREDENTIAL SERVICE PROVIDER)
RELYING PARTY
AUTHORITATIVE PARTY - Identity - - Personal Attributes -
AUTHORITATIVE PARTY - Identity - - Personal Attributes -

provide an overview of the reference models supported by the Federated Authentication and Brokered Authorization Model.

1. The identity ecosystem can be supported by a simple model having three major service components: credential services, permission services and identity services.
2. This model can be elaborated to support a broad set of use cases, architectures and implementations.
3. All services (credential, permissions and identity) can be brokered in a way that ensures security and privacy.
4. Each component can be independently operated (but is subject to trust framework requirements or equivalent).
5. The model supports a multiplicity of standardized service providers to allow for choice between service providers and redundancy (no single point of failure).

Technical next steps

DIACC will undertake the following steps to continue to move forward the process of establishing a technical model and architecture:

1. Identify and publish a set of protocol specifications.
2. Execute additional proofs of concept to test the Federated Authentication and Brokered Authorization Model in multiple use cases and in multiple service contexts to ensure its broad applicability.
3. Continue to leverage and learn from models and recommendations of similar efforts around the world (United Kingdom, United States of America, Estonia and New Zealand).
4. Harmonize existing considerations into a set of guiding principles.
5. Translate the guiding principles into a set of policies to form the basis of a trust framework and align them with the prior work developed by the public sector.

CATALYZE. FACILITATE. STIMULATE.

Canada is ideally situated to implement a digital identity strategy. Canada and its provinces, territories, municipalities and private sector have a history of successfully undertaking transformative projects that benefit all citizens. In the past, we built the great trans-continental railway, the TransCanada highway, our national and provincial parks systems, and a number of leading transaction technologies such as those delivered by Interac.

Developing a robust digital identity ecosystem is no more complex, and Canadians are already recognized internationally as leaders in this industry. Governments and companies from around the world already seek the advice of Canadians abroad such as Kim Cameron, Kaliya "Identity Woman" Hamlin, Pam Dingle and Dick Hardt when considering which digital identity technologies to adopt internationally.

> "It can be tough for Canadians with disabilities to get to a bank branch in person, so we'd like to see this online concept move forward. Providing more services through accessible secure digital channels could make routine activities much easier for people with impaired mobility and vision. Let's remove barriers and level the playing field."
>
> —Gary Birch, Executive Director, Neil Squire Society

Cameron's *7 Laws of Identity*[26] have become foundational work for guiding IT system design. Similarly, the seven principals of privacy by design developed under the leadership of Dr. Ann Cavoukian as Information and Privacy Commissioner of Ontario have been recognized by the International Conference of Data Protection and Privacy Commissioners as an essential component of fundamental privacy protection. The federal, BC and Alberta privacy commissioners have published a document titled Getting Accountability Right.[27] This document and the accountability approach is important and relevant because it emphasis the need to have strong data governance and a comprehensive privacy program in place in order to enable trust between entities sharing information. Commissioners across Canada are collaborating on an approach to harmonizing the various legislative regimes and to encourage a due diligence, harmonized approach across the private and public sectors. We are leaders.

Canada must leverage its considerable knowledge base in the realm of digital identification. The public and private sectors need to adopt digital identification and integrate it into their operations. Individuals need to be informed of the improvements in security and convenience that digital identification brings and adopt it into their daily activities.

Digital initiatives across Canada

Governments and other organizations across the country are working at many levels to ensure that Canadians have access to secure, reliable and private digital services. The following is a list of some current activities and interests. For details about each item, please see Appendix F.

Federal government initiatives

- Digital Canada 150
- Secure Access to Government of Canada services online via SecureKey Concierge and GCKey
- Canada's Digital Interchange

Provincial Government initiatives

- British Columbia Services Card
- New Brunswick in pursuit of digital leadership
- Ontario's One-Key and Go-Secure solutions

Pan-Canadian councils

- Joint Councils of the Public Sector Chief Information Officers Council (PSCIOC) and Public Sector Service Delivery Council (PSSDC) and the Identity Management Sub-Committee (IMSC)

Education and community building

- Monthly identity networking workshops by DIACC

[26] See: http://bit.ly/1ySXDn8

[27] See: http://bit.ly/14WQggW

APPENDICES

Appendix A—Proof of Concept

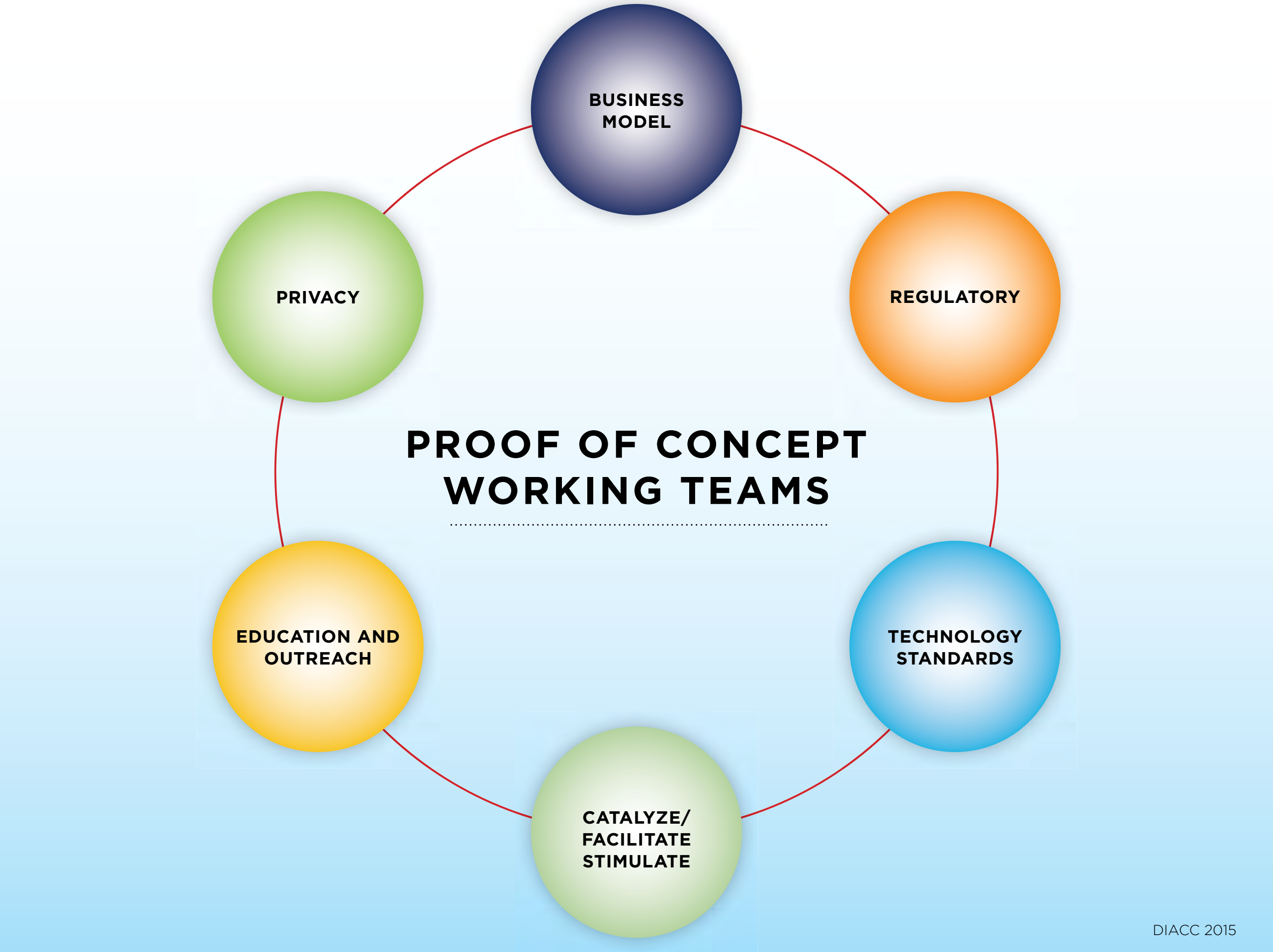
As part of the investigation into the future of digital ID and authentication (DIA), DIACC members decided to undertake a proof of concept that would provide a blueprint for moving forward. The proof of concept needed to demonstrate a highly visible solution that could be quickly and cost effectively implemented using existing technologies while touching upon some of the regulatory and policy considerations currently identified as posing a hindrance to the widespread adoption of DIA. The proof of concept also had to be representative of many broader applications and the underlying processes had to be adaptable to many sectors of the economy.

Problem statement

Canadians are currently limited by the need to present physical ID and provide "wet signatures" to open new accounts with Canadian financial institutions.

Proposal

Develop a proof of concept to open new financial accounts entirely online by leveraging new technology including, but not limited to, attribute sharing, data imaging and radio-frequency identification (RFID) technology.



DIACC members collaborated for six months to support the modeling deliverables. Supporting activities included:

- a review of general considerations and key principles

  a review and comparison of potential existing models
- the identification of a model that could deliver an effective solution and proceeding activities required for moving towards realization

Execution

DIACC organized contributing members of the Council into working teams focused on defining and identifying the elements required to develop and implement a supporting framework and ecosystem for digital ID.

As part of the proof of concept, DIACC members decided to create a working demo. The objectives of the demo included the following:

1. Demonstrate a user experience that provides context for elevated discussions and feedback. The demonstration will illustrate a likely user experience for Web service and a mobile agent.
2. The demonstration will showcase as complete a solution model as is feasible today. The demonstration identified future technical issues and constraints that might limit stakeholders adopting the proposed technical solution and clarify any prerequisite technical activities required before implementation.

The demonstration included the following:

- Participation of DIACC's financial institution members so as to elaborate on the solution's implied capabilities and constraints for our financial institutions
- Participation of intermediaries to demonstrate scalability and support multiple data validation sources
- Participation of DIACC's members as authoritative parties
- Details about how the solution aligns with the proposed legislative and regulatory environment
- Details about how privacy considerations are effectively addressed by the solution
- Details about how the solution is vendor neutral and supports open standards
- Delivery (of the demonstration itself) within a short period of time to ensure that the impact to DIACC member resources was limited and momentum was maintained
- Availability of the demonstration infrastructure over several months to support DIACC activities, building awareness and promoting interest in the Council

Demo solution model

DIACC members were asked to take on various roles within the process. One of the intentions of the proof of concept was to demonstrate how multiple organizations could act as relying parties and authoritative parties, and perform different functions within the core DIA architecture/ platform.

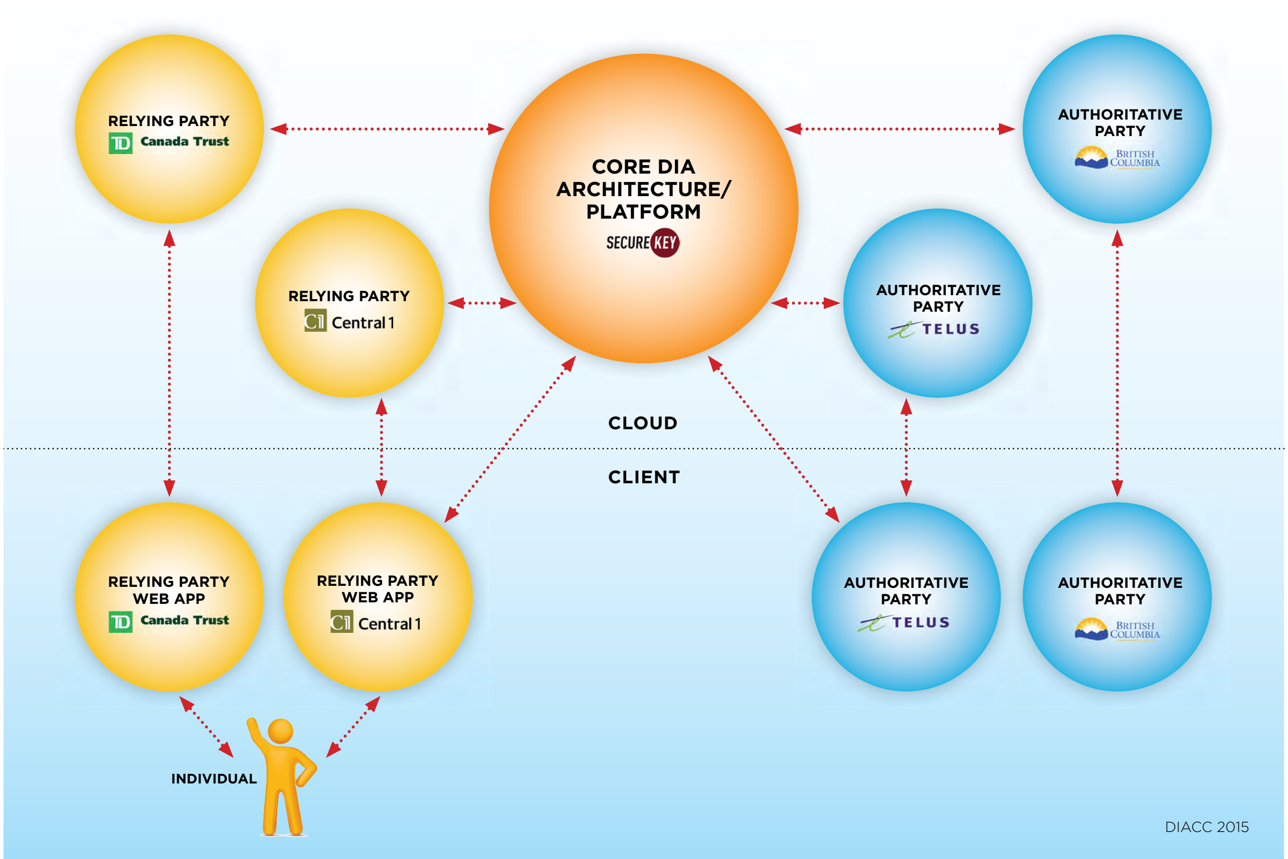
For demo purposes:

- TD Canada Trust and Central 1 acted as relying parties
- SecureKey acted as the core DIA architecture platform
- the Government of British Columbia and TELUS acted as authoritative parties

Demo use case

1. User follows flow at a financial services organization's Web page for online services in order to open a new account online. For the demo, Central 1 and TD acted as the demonstration financial institution relying parties.
2. The financial services "open account online" Web flow arrives at a purely online option with a "Select Identification Verification Method" options menu.

PROOF OF CONCEPT



3. The selector page represents the user interface with the instance of SecureKey Concierge acting as intermediary for the demo.
4. User selects TELUS Mobile Connect ID service option:
   - TELUS Mobile Connect ID Service pop-up is prompted by user selection.
   - User enters their mobile number or scans QR code with TELUS Mobile Connect Mobile Application hosted by SecureKey.
   - The user identification is successfully authenticated by the Mobile Connect application interfacing to the TELUS wireless service identification service.
   - Using the TELUS Mobile Connect application on their mobile device, the user views and consents to the attribute request.
   - The Mobile Connect application will conduct back-end calls to the TELUS customer identity authorization service and to an authoritative party database. For the proof of concept, this database was mocked up by SecureKey.
   - The consented attributes are delivered via the intermediary to the relying party financial institution.
   - The financial institution receives the attributes from the trusted source and proceeds with the account opening flow.
5. User selects BC Services Card option.
   - User selects BC Services Card option.
   - User is redirected to BC Services Card login website.
   - User is prompted to tap their card on either a USB card reader or an android mobile device with near field communication (NFC) capabilities.
   - User selects a method and taps their card.

- BC Services Card data is read from the card and authenticated with several back-end systems.
- User is prompted to enter their passcode.
- User enters their passcode and it is validated by the back-end system.
- User is prompted to confirm the sharing of their identity attributes from the BC Services Card system to SecureKey Concierge.
- User confirms the information sharing.
- Identity attributes and assurance level are provided to SecureKey Concierge.
- The consented attributes are delivered via the intermediary to the relying party financial institution.
- The financial institution receives the attributes from the trusted source and proceeds with the account opening flow.

Appendix B—Electronic Confirmation of Identity

This method of ascertaining a person's identity consists of two parts:

1. Electronically confirming the accuracy of person's identity information using an accredited authoritative source
2. Ensuring the identity information being confirmed relates to the person making the claim (i.e., not to another person)

These two parts, as described in the proposed method above, relate to two key objectives that must be met when ascertaining identity:

- **Objective 1: Accuracy of identity information.** Identity information about an individual must be accurate, complete and up to date. Accuracy ensures that the identity information represents what is true about the individual and the individual truly exists (i.e., not a fictional or synthetic identity). Confirming the accuracy of information is also referred to as identity validation.
- **Objective 2: Linkage of identity information to the individual.** Identity information, once confirmed as accurate, must relate to the individual making the claim. Linkage ensures that identity information is not being fraudulently used by another individual. Ensuring the linkage of information is also referred to as identity verification.

Together, when these objectives are met, they can provide a level of assurance that an individual is actually who they say they are and be relied on as a digital alternative to an in-person and/or document-based identity-proofing process.

Appendix C—Consumer-driven Assumptions

1. Consumers will want to determine what private data can be obtained by other parties—namely, the relying party and the authentication service.
2. Not all private data may be given to the relying party, but private data will be supplied that is required for undertaking a legitimate business requirement (need to know) or that is required by law may. Some sensitive (secret) data must remain hidden to third parties (relying parties and authentication services). By default, the relying party does not gain access to the consumer's sensitive data.
3. Consumers will want strong security (integrity, confidentiality and privacy) on sensitive data such as authentication credentials.
4. An intermediary may be required between credential service providers and the relying party when a relationship has not been previously established. This intermediary would offer the authentication service to the relying party (authenticate consumers to relying party upon request and link transaction to authentication).
5. A credential service provider may also play the role of credential authentication service if a relationship between the relying party and the credential service provider already exists).
6. All parties involved must ensure confidentiality, authenticity and integrity of transactions.
7. The relying party will not always have established trust with the consumers prior to the transaction.
8. Credential service providers will not always have prior direct relationship with relying parties.
9. Federation and trust:
   - Trust must be established between consumers and credential service provider prior to transactions.
   - Trust must be established between the authentication service and relying party prior to transactions.
   - The authentication service must trust CI.

Appendix D—Levels of Assurance

Treasury Board Standard on Identity and Credential Assurance[28]

Identity assurance levels

Level	Description
1	**Very high confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause serious to catastrophic harm.
2	**High confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause moderate to serious harm.
3	**Some confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause minimal to moderate harm.
4	**Little confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause nil to minimal harm.

Credential assurance levels

Level	Description
1	**Very high confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised.** Compromise could reasonably be expected to cause serious to catastrophic harm.
2	**High confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised.** Compromise could reasonably be expected to cause moderate to serious harm.
3	**Some confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised.** Compromise could reasonably be expected to cause minimal to moderate harm.
4	**Little confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised.** Compromise could reasonably be expected to cause nil to minimal harm.

[28] S See: http://bit.ly/1OBxBMu

Appendix E—Ecosystem, Privacy and User Experience Requirements Met by the Federated Authentication and Brokered Authorization Model

Ecosystem requirements:

- Simple integration scenarios
- Economic model for all actors
- Workable billing and reporting model
- Easily scalable to other use-cases involving other entities and data

Privacy requirements:

- Pseudononymous identifiers provided to each service (i.e., no globally unique user identifiers are provided by DIA platform)
- User consent is required to authorize sharing of data
- Consent screen is independent of application requesting access
- Minimized knowledge of user activities for each actor or system component

User experience requirements:

- Consent screen displayed to the user (consent screen may allow for authorization of long term access to data, depending on use-case requirements)
- User can identify themselves to a data service once to enable multiple apps (accomplished by binding a user identification to a data service via an authentication service)
- Compatible with both Web and mobile (application program interfaces) become the focus because they can support either Web or mobile experiences)
- Minimizes delays due to Web redirects, particularly in mobile cases (when this doesn’t conflict with security requirements)

Appendix F—Digital Initiatives across Canada

Government of Canada initiatives

Digital Canada 150

Digital Canada 150 represents a comprehensive approach to ensuring Canada can take full advantage of the opportunities of the digital age. It envisions a country of connected citizens armed with the skills they need to succeed. Based on five pillars—connecting Canadians, protecting Canadians, economic opportunities, digital government and Canadian content—the Digital Canada 150 program provides clear direction and can act as a catalyst for Canadian businesses and consumers.

Some of the key initiatives within Digital Canada 150 have been to strengthen the *Personal Information Protection and Electronic Documents Act* to better protect the online privacy of all Canadians, and to create new authentication services for consumers, including the credential broker service and GCKey (an electronic credential that allows you to communicate securely online with certain government programs and services), which make it easier to manage and secure online usernames, identities and passwords. Digital Canada 150 has committed the Government of Canada to becoming be a leader in using digital technologies to interact with Canadians, making it simpler and quicker to access services and information online.

Digital Canada 150 must stay current. Industry Minister James Moore says the strategy's most important passage falls in the last paragraph on the last page: "It is imperative that we keep our plan current because, in the digital world, change is the only constant. We are committed to continuously updating Digital Canada 150, adapting to better serve Canadians."

Secure online access to Government of Canada services

Sign-in partners are organizations that have partnered with SecureKey to enable their customers to use their online credentials, such as card numbers or user names and passwords, to access Government of Canada services. Sign-in partners currently offered include BMO Financial Group, CHOICE REWARDS MasterCard, Scotiabank, TD Bank Group and Tangerine.

The GCKey service is provided by the Government of Canada to allow individuals to securely conduct online business with various governmental programs and services. A GCKey is a unique credential that protects communications with online government programs and services.

Provincial government initiatives

British Columbia

BC introduced the BC Services Card in February 2013. The new card is designed to make it easier for BC residents to access provincial government services. Most residents will be able to use just one card:

- as a Care Card
- as a driver's licence
- to access services that need a photo ID

The BC Services Card takes advantage of modern card technology that provides better security features. The card now includes a photograph of the beneficiary, anti-forgery features, identity proofing and an expiration date, and utilizes chip and PIN technology similar to what Canadian banks use. Plus, using ICBC's existing identity proofing and renewal processes will keep everyone's personal information more secure and help prevent fraud like identity theft or misuse of the BC Services Card will provide access to government services—starting with provincial health care services for eligible B.C. residents. It can also be used anywhere you currently need to present identification, such as to open a bank account or check into a hotel.

The card may be used to access different services, while protecting the privacy of the user. For example, a health care provider will not be able to see a patient's driving record, while a police officer or ICBC employee will not have access to an individual's health records.

In the future, the card will be able to be used to access other government services online or in person.

Every BC Services Card has a chip embedded in it—similar to the ones used by debit cards in Canada. In the future, chip technology will allow individuals to access a service by tapping their card on a card reader. It will recognize the unique chip and validate the user's identity to the service provider. It is important to note that the card does not store any personal information like health or driving records. Access to an individual's records is protected by a passcode, similar to the personal identification number (PIN) associated with a bank card.

To get a new BC Services Card, eligible British Columbians simply enrol when they are renewing their driver's licences. The province has issued more than 2 million BC Services Cards and expects to roll it out to nearly all residents within five years (2018).

New Brunswick

There is a lot of interest in New Brunswick in regaining leadership in digital services. The private sector is an active leader in this initiative. In summer 2014, more than 120 local leaders from the public and private sectors gathered as they launched a campaign called Towards a Digital Society to build a digital future for New Brunswick through the adoption of digital ID and enabling infrastructure.

The newly elected government is currently conducting an extensive strategic program review that contemplates significant transformative change. Although New Brunswick has not yet taken a position on digital ID, work continues to develop prototypes and continue the dialogue on what the digital future could be.

Ontario

External authentication and identity

The Government of Ontario operates a public authentication solution called ONe-Key. ONe-Key is a double-blind solution that authenticates a user but requires each program area to independently identify the client to deliver service. There are more than 15 programs that leverage One-Key's capabilities, including Ontario Student Assistance Program (OSAP) and ONe-Source for Business Portal.

For applications where risks are manageable through process and technical controls, Ontario leverages fact-based identification to deliver programs. This approach is typically leveraged where transactions are so infrequent that the creation and maintenance of an "account" is impractical.

Ontario is currently exploring opportunities to leverage new and existing technologies that will enhance client experience and will assist the province to move new programs online.

Internal authentication and identity

The Government of Ontario manages an identity and access management platform called Go-Secure. Go-Secure enables internal employees, extranet users and agents of the government to securely access government applications.

EHealth Ontario has introduced an identity and access management system and set of associated processes called ONE ID. It is based on an infrastructure of trust that connects clinics, hospitals, pharmacies and other points of care. This means that eHealth Ontario relies on trusted individuals within each organization to sponsor and verify the identity of each individual who will be registered and enrolled for e-Health services available through eHealth Ontario. Once enrolled in ONE ID, individuals are able to access services in a highly secure, controlled and efficient manner. ONE ID's enhanced privacy and security safeguards help protect patient and registrant information. One ID also allows use of the same digital identity to access multiple eHealth services hosted by eHealth Ontario, thereby reducing the number of IDs and passwords a user must manage and remember.

Conferences

IdentityNorth

IdentityNorth is the leading event for individuals and organizations interested in digital identity and the digital economy. It is an important platform to share the ideas and knowledge that will drive Canada's digital future. The conference delivers high-value content through its subject matter experts, keynotes and an "unconference" day—a participant-driven event where attendees build the agenda and lead inspiring and insightful sessions on contemporary identity topics.

Education

It is important to educate Canadians about the benefits of digital identity from a privacy and identity fraud standpoint—not simply from a convenience standpoint. Secure digital identification is more secure than traditional paper-based identity methods, which can be easily forged, are often photocopied and stored in an unsecure manner, and verified by persons without any special training in detecting identity fraud (e.g., bank teller or liquor store clerk).

Building a community

Another way to educate citizens is to build a community of likeminded individuals and organizations across all business sectors, the public sectors and all geographic regions. These people will be the standard bearers and ambassadors of digital identity. In addition, they will be the innovators and developers of new technologies and services that have been previously unattainable, or not even contemplated or considered before the establishment of a digital identification ecosystem.

Critical mass is essential for any endeavour to take off and the identity community has been growing in Canada but needs to grow larger and more quickly.

DIACC has taken a first step in this regard with a series of monthly identity networking events in cities across Canada. Over the last few months several hundred leaders in the identity field representing the public and private sector, the largest banks and the newest start-ups have come together to discuss their successes, challenges and vision for the future.

Appendix G – Summary of Stakeholder Responses

The DIACC Stakeholder Team sought comments and views from a variety of consumer and user groups across Canada about the proof of concept (POC) "How to Open a Bank Account Online without a Prior KYC Experience." Nine organizations were selected for their expertise in consumer affairs and/or financial services, and telephone interviews were conducted with representatives of these groups between May and July 2014. The objective of the consultation was to identify benefits and areas of support, as well as potential issues that could be addressed.

Groups interviewed

- CARP (formerly the Canadian Association of Retired Persons), Toronto
- Consumers Council Association of Canada
- Consumers Council of Canada
- Financial Consumer Agency of Canada, Ottawa
- First Nations Bank of Canada, Saskatoon
- Neil Squire Society, Vancouver
- Option Consommateurs, Montreal
- Public Interest Advocacy Centre, Ottawa
- St. Christopher House, Toronto

Summary of stakeholder comments

The stakeholder representatives identified potential benefits of the POC, including:

- greater convenience for consumers, especially those living in remote and rural communities
- a wider choice of banking options generally
- better access to banking services for disabled people and those with mobility issues
- the opportunity for financial institutions to attract new customers and provide additional products/services

The representatives interviewed also raised concerns or questions about:

- security of the digital ID and authentication processes and system
- the potential for identity theft or fraud
- consumer protection and liability issues if something goes wrong
- the extent and language of online disclosure

Summary of Stakeholder Team response

The DIACC POC team has been considering the issues and concerns raised by the stakeholder representatives as part of a broader set of requirements and legislative considerations. Concerns that are within the scope of the POC are being addressed through the following activities:

- The DIACC Technical Team has identified a technical framework that takes into account a broad range of security and privacy considerations, including the issues and concerns raised in the interviews.
- The DIACC Regulatory Team has identified the regulatory and legislative changes required to ensure compliance with laws and regulations, and has also identified opportunities to update legislation to reflect advances in identity management technology.
- The DIACC Privacy Team had open and transparent consultation with various privacy commissioners to ensure the proposed solution adheres to and, in some cases, strengthens Canadian privacy laws and desires.

About DIACC

The Digital Identification and Authentication Council of Canada is developing Canada's ecosystem for Digital ID to enable full and secure participation in the global economy.

Created as a product of the Department of Finance's Task Force for the Payments System Review, the DIACC is the 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 in the global digital economy. DIACC members include representatives from both the federal and provincial levels of government as well as private sector leaders.

We are committed to unlocking economic opportunities for Canadian consumers and businesses by providing the framework to develop a robust, secure, scalable and privacy-enhancing digital identification and authentication ecosystem that will decrease costs for everyone while improving service delivery and driving GDP growth.

DIACC's members and advisors include leaders from both the federal and provincial levels of government as well as representatives from small and large businesses, charities and privacy commissioners.

We operate transparently and participation is open to all Canadians. Our current membership includes all of Canada's major financial institutions and credit unions, telecommunications companies, departments within the Canadian federal, provincial and municipal governments, and technology providers.

Our mission statement

- The Digital Identification and Authentication Council of Canada shall catalyze changes and set the strategic direction for digital ID and authentication for the public and private sectors in Canada.
- Develop and recommend harmonizing policies, standards and regulatory changes with international benchmarks that further the strategic direction such as standardization of levels of assurance in digital identity and liability models for digital ID and authentication.
- Enforce the minimum requirements necessary to enter the digital ID and authentication ecosystem.
- Promote interoperability between participants in the digital ID and authentication ecosystem, and with international digital ID and authentication schemes.
- Provide a forum to foster collaboration among digital ID and authentication ecosystem participants, to formalize existing standards and to create new ones.
- Provide operating guidelines to the marketplace and set certification processes to ensure that digital ID and authentication is known for delivering efficient, secure, safe, reliable, privacy-enhancing transactions.
- Ensure that Canada's digital ID and authentication ecosystem is accessible to all.
- Promote public understanding and accelerate the adoption of digital ID and authentication in Canada.

Members of the DIACC at the time of this report include:

- BlackBerry
- BMO Bank of Montreal
- Canada Post
- CIBC
- Credit Union Central of Canada
- Deeth Williams Wall
- Desjardins Group
- Equifax
- Equitable Bank
- ForgeRock
- Government of Canada
- Interac
- Notarius
- Online Business Systems
- PacificEast
- PlaceSpeak
- Province of British Columbia
- Province of New Brunswick
- Province of Ontario
- PwC
- Rogers
- Royal Bank of Canada
- Scotiabank
- SecureKey
- Sierra Systems
- Simeio Solutions
- TD Bank
- TELUS
- Thirdstream
- Thoughtwire
- Ticoon
- TransUnion
- Trulioo
- 2Keys

For more updates from the DIACC, visit www.DIACC.ca and follow us on on Twitter **@DigitalCdns**.

Contact

Aran Hamilton, President, Digital ID and Authentication Council of Canada **AHamilton@DIACC.ca**
David Richards, VP, Director of Operations, Digital ID and Authentication Council of Canada **DRichards@DIACC.ca**

DIACC