Canada's Digital ID Future - A Federated Approach

Spring 2018

ASSOCIATION DES BANQUIERS CANADIENS

CANADIAN BANKERS ASSOCIATION

Digital ID is the challenge of answering "Who are you?" with a high degree of certainty, without resorting to face-to-face interaction and the exchange of physical documents.

Countries around the world are crossing the electronic frontier and exploring the benefits of integrating digital identity systems. With the growing number of Canadians accessing services and businesses online and the increased usage of mobile phones, Canada is in a position to move forward with a more robust digital identity system. In this brief, we highlight why Canada needs a digital identity system, how other countries have made progress in this area and the lessons we can learn from those experiences to build a system in Canada.

Digital Identity Defined

Identity is the representation of who you are. A person's identity is composed of different attributes such as name, date of birth, address and citizenship. Historically, the way we established our identity is through physical documents (e.g. driver's license, passport, ID card), sometimes supplemented with some form of physical verification (typically a signature). In our increasingly pervasive digital world, our ID can also include additional attributes like usernames and passwords, as well as physical factors like the SIM card in a mobile phone. A digital ID is a way for people to identify themselves electronically without the need to present physical documents.

It is important to differentiate between digital *identification* and digital *authentication*. Digital authentication is something most of us do every day – logging on to our favourite social media site, signing into an account with our preferred ecommerce retailer, or even accessing our mobile device through a thumb scan. Authentication is the act of proving that the person accessing my account or device is me, usually through a PIN, password, biometric identifier or other form factor. Authentication is designed to answer the question "*Is that you?*" Identification, by contrast, is more complex. Identification is intended to answer the question "*Who are you?*" Digital ID is the challenge of answering "Who are

The public and private sectors shoulder the costs associated with identity collection, and sometimes these efforts are duplicative.

you? with a high degree of certainty, without resorting to face-to-face interaction and the exchange of physical documents.

Why Canada Needs a Digital Identity System

All Canadian stakeholders – citizens, businesses and governments – stand to gain in several ways from an effective digital ID system.

- **Cost Savings** – The public and private sectors shoulder the costs associated with identity collection, and sometimes these efforts are duplicative. For the private sector, the process of verifying identity is costly for financial institutions and their customers with Know Your Client (KYC) and Anti-Money Laundering (AML) compliance accounting for billions of dollars in expenses globally[i]. Approximately 1.5 million Canadians switch banks annually[ii] , and when they open an account with a new financial institution, they must present ID to establish their identity. For the public sector, on the other hand, approximately 5 million Canadian drivers need to replace expiring physical licenses annually, creating a time and cost burden for citizens and governments.[iii] Because most of these processes involve physical ID, they are cumbersome and inefficient – and therefore, expensive.

- **Fraud Reduction** – Criminals continue to exploit weaknesses in current physical ID systems. An effective digital ID regime can reduce Canadians' exposure to financial fraud and identity theft. A report by TELUS noted 74% of businesses are affected by online fraud and fraud-related crimes cost Canada between $15B and $30B annually. Further, the percentage of exposed identities

A digital ID system enhances privacy and puts greater control of identity back into the hands of the consumer.

grew by 23% in 2015[iv] and continues to increase annually. Of particular concern is the rise of synthetic identity fraud where bad actors combine real and fabricated information to defraud businesses and governments. In a report on synthetic ID fraud, weaknesses in existing legacy systems were being exploited where creating synthetic ID is becoming easier.[v] The current limitations to sharing identification information securely between government agencies' physical identity cards create an opportunity for fraudsters to exploit the system.

- **Improved Regulatory Compliance** – Monitoring and reporting complex transactions can be more efficient with a proper identity management system in place. For example, in Ontario the provincial Office of the Auditor General's 2015 annual report noted that in 2014/15 ServiceOntario handled more than 37.5 million transactions, 70% of which were conducted through in-person service centres.[vi] Numerous challenges were identified with current processes involving physical identification, including missing signatures, improper financial information, and thousands of cards in circulation for dead people. Reliance on face-to-face interactions coupled with the inefficiencies of physical documentation prompted the Auditor General to recommend that the government find ways to increase the public's use of online services to reduce costs and lower the risk of fraud. ServiceOntario subsequently submitted a plan in July 2017 for a policy framework for a single digital ID business case.[vii]

- **Privacy Enhancing -** Privacy and security of personal identification is a growing concern. A digital ID system enhances privacy and puts greater control of identity back into the hands of the consumer. Unlike physical documents, digital ID can be standardized and used

More and more countries are seeing the need to find a solution to the identity challenge

between entities with the ability to adapt by adding new information. Moreover, only one version of your identity *exists, significantly reducing the potential for* misinformation, identity theft or the use of outdated data that does not reflect your current identity.

- **Future Ready** – Canada is among the jurisdictions studying the effects of open banking systems now in place in Europe, the UK and Japan, to consider how enabling third-party access to customer banking data could work here. Digital ID must be solved before we move into open banking. Without an agreed upon digital ID framework, information can be more easily accessed by the wrong individuals. For example, in a regime where third parties can access bank accounts and send e-transfers, having a standard to ensure that the correct individual is in fact sending the funds is crucial to mitigate fraud and financial losses.

Digital Identity Systems – Global View

Digital ID systems are evolving rapidly around the world. The ID2020 initiative, in which the UN is a partner, says "Identity is foundational for political, economic and social opportunity."[viii] More and more countries are seeing the need to find a solution to the identity challenge. Estonia and India are two countries that have made strides in digital ID. Their experiences are instructive for Canada.

Digital Identity in Estonia – Building a Smart Nation

Estonia is frequently cited as having one of the most advanced digital ID frameworks, where all citizens have a digital ID to

Digital ID was used 80 million times for authentication and 35 million times for digital transactions in a nation of only 1.3 million people.

access government services. Estonia began its digital ID transformation by establishing a regulatory framework with two foundational pieces of legislation:

- The *Identity Documents Act* ensured that all Estonians were issued "smart" ID cards. The ID card was introduced with two separate PINs: the first one for authentication and the second for digital signatures.

- The *Digital Signatures Act* (DSA) provided the legal foundation for accepting digital signatures through the use of digital ID cards and created a certification registry to verify digital ID card digital signatures. This Act stated digital signatures are equivalent to handwritten ones and the public sector must accept digitally signed documents.[ix]

The private sector also adopted the digital ID framework. The legislation allowed the financial services industry to use digital ID to offer banking and other services. Widespread adoption of digital ID by the private sector generated broad social awareness and enhanced the acceptance of the new system. Estonia built X-Road, the data exchange layer that allows the public and private sector to securely exchange data and to ensure the information is compatible and up to date, to allow people to access a variety of services using their digital ID. Estonia's ID cards are now widely used across a variety of platforms including healthcare, electronic banking and even voting. By 2014, digital ID was used more than 80 million times for authentication and 35 million times for digital transactions – a significant achievement for a nation of only 1.3 million people.[x] The improved efficiencies resulted in savings estimated to be the equivalent of 2% of Estonian GDP. [xi]

India has grown its database to cover 95% of the population.

Digital Identity in India – Nationwide Identity Management

India developed a digital ID system to create a unified nationwide identity management program. The absence of a truly national identity management regime led to problems of social exclusion and limited access to government services. As a first step, in 2009, the Government of India established the Unique Identification Authority of India (UIDAI). It directed the Authority to create a reliable, verifiable and cost effective identity management system, now known as *Aadhaar*.[xii]

Similar to Estonia, the Government of India developed a legal and regulatory framework to recognize digital ID. In 2016, the government enacted the *Aadhaar Act*, which authorized the UIDIA to manage all aspects of Aadhaar and made it responsible for ensuring that citizens' identity information is secure. While not mandatory for identification, the Indian government has made enrolment in Aadhaar mandatory to access any government subsidy, benefit or service. As a result, adoption of the new system has been strong. India has since grown its database to more than 1 billion users covering approximately 95% of the Indian population.[xiii]

The Indian government has leveraged Aadhaar to address social and economic policy goals. One example is India Stack, which is a series of secured and connected systems designed to store personal data like bank accounts and tax filings. These can be accessed and shared via Aadhaar.[xiv] This, in turn, has formed the basis of an "e-KYC" system that enables financial institutions to digitally identify a customer. Overall, the national digital ID system helped save the government about $9 billion USD by improving efficiency and reducing fraud.[xv]

Canada will need to create an environment that enables a digital ID system to be built.

Digital Identity Systems – Lessons for Canada

While Estonia and India took different paths and used different technologies to implement a digital ID solution, there are some commonalities in their approaches that provide valuable lessons for Canada. Both countries underwent a complete digital transformation following the same core public policy roadmap:

- They ensured that the concept of a digital ID was enshrined in legislation. Policy makers recognized that for business and government to accept digital ID, they would need certainty that it met legislative and regulatory requirements for customer identification.

- They recognized that the government would need to act as a catalyst to bring a digital ID system to market by building the system directly and allowing industry to expand upon that framework to develop more efficient and secure ways to execute transactions.

- They developed the necessary digital information infrastructure to ensure citizens, businesses and government are able to use the Digital ID system.

Canada is clearly a very different country than either Estonia or India. As a mid-sized, highly-developed economy, it has a more established private sector that it can leverage to create a digital ID architecture and roll it out to residents. The lessons from Estonia and India, however, are instructive from a public policy perspective. To give effect to a digital ID system, Canada will need to follow the same underlying path as both of those countries – it will need to build a legislative/regulatory environment that enables a digital ID system to be built,

A key factor in establishing a robust Canadian digital ID system is modernizing the regulatory framework that both accommodates and encourages innovative digital ID solutions.

accessible to all, and that empowers industry and government to accept the digital ID as it comes to market.

Creating a Roadmap to Federated Digital ID in Canada

A key factor in establishing a robust Canadian digital ID system is modernizing the regulatory framework that both accommodates and encourages innovative digital ID solutions. The federal government has taken an initial step by outlining key principles in its Inclusive Innovation Agenda, including the need to compete in a digital world and the imperative to make doing business easier. The development of a national digital ID framework is tightly aligned with these key principles and is essential for Canada's future participation in the digital economy. While the steps taken by the government are encouraging, further federal action is needed to address any regulatory roadblocks that could hinder or prevent Canadians from widely adopting digital ID. What follows are a set of recommendations to ease the establishment and adoption of such a system here.

Harnessing the Power of the Private Sector

Canada's highly developed private sector can create an effective and innovative digital ID system without the cost and risk of building a large, centralized system from scratch. Currently Canada's identification model is decentralized, with isolated systems holding different attributes of an individual's identity. In Ontario, for example, the Ministry of Health issues health cards, the Ministry of Transportation issues driver's license and banks and other financial institutions manage an individual's financial information. Yet, there is no linkage or connection between these separate attributes of data to be able to identify someone.

Canada's strong financial institutions must play a key role. The World Economic Forum stated in its report that financial institutions should champion efforts to build digital ID systems and lead the creation and implementation of identity platforms.

Canada has the opportunity to create an interconnected or "federated" digital ID framework between government and private sector whereby a person's electronic identity and attributes are stored across distinct but linked identity management systems. By using a federated system, Canadians could verify their identity electronically using a combination of different attributes through the government (like a driver's license), banking log information and biometrics such as fingerprints or facial recognition.

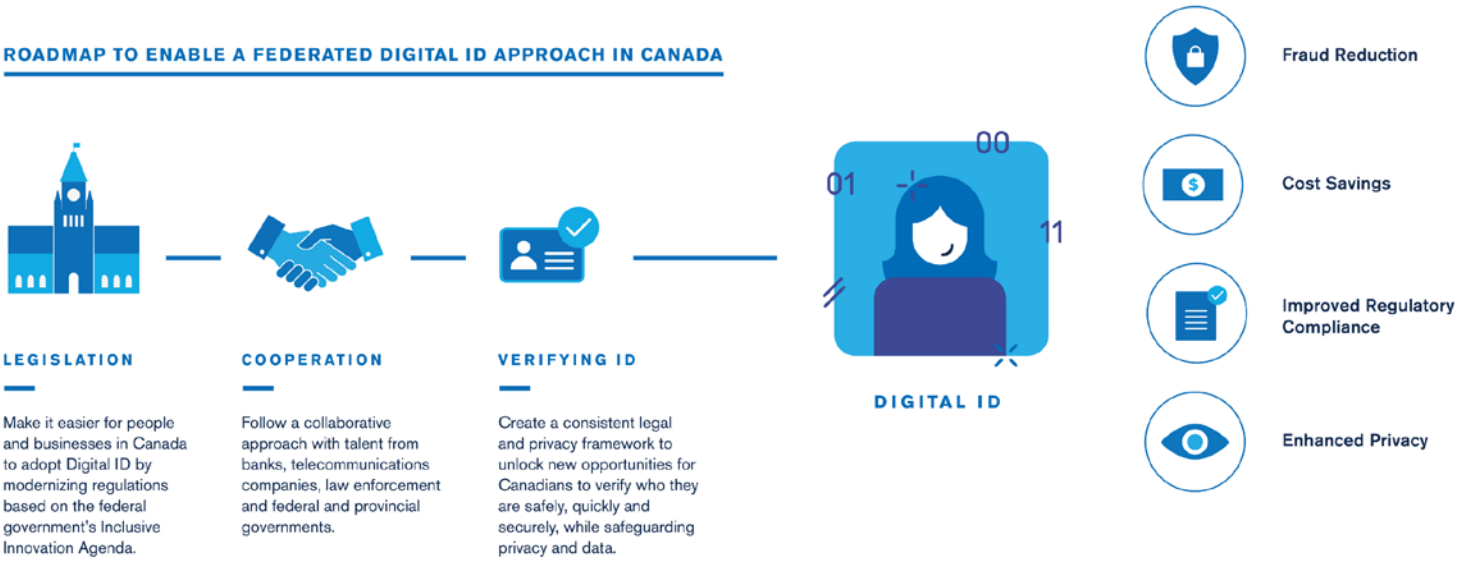
The advantages to the federated digital ID system are clear for Canada. Unlike a centralized identity framework that puts the control of identity under one key player, a federated identity system leverages multiple systems, eliminating reliance on a single service provider. In other words, there is no single point of control or failure that can compromise the entire system. A federated model would also align with Canada's federal structure by creating linkages between provincial and federal government identity management systems. The decentralized network also reduces the risk of fraud by eliminating any "honeypots" of data that can be compromised. This ability to verify identity through a single, streamlined view offers more privacy for individuals while enabling faster onboarding and transparency for customers, businesses and governments.

Canada's strong financial institutions must play a key role. The World Economic Forum stated in its report that financial institutions should champion efforts to build digital ID systems and lead the creation and implementation of identity platforms.[xvi] Financial institutions and banks are held to a high standard to maintain and protect personal information and are subject to rigorous oversight. Canadians trust banks to hold and maintain personal data accurately and securely. Banks also have the infrastructure to operate across provinces and internationally to underpin digital identity solutions in Canada. Banks have been providing "letters of reference" in paper form for their clients for

centuries. With the acceleration in technological development, the natural evolution of these letters of references is to move to digital form. Greater clarity in the *Bank Act* around digital ID services would better support banks in exploring the full scope of opportunities in this area.

Enabling Use of Digital Identity Across the Economy

Many businesses and government agencies have legislative and regulatory requirements they must adhere to when establishing the identity of their clients. For digital identification to be fully embraced, legislation and regulation such as the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* will need to ensure that businesses can accept digital identification. While some provisions exist currently for identification through non-face-to-face methods, broader and more robust provisions for the use of digital identification would ensure people, businesses and governments are able to benefit from digital identification systems, and would send a strong signal that Canada is embracing the digital economy.



In today's connected era, physical documentation causes unnecessary friction, while also creating opportunities for fraud and identity theft.

Moving Canada ahead with Digital Identity

Canada's economy is undergoing a digital transformation. In today's connected era, physical documentation causes unnecessary friction, while also creating opportunities for fraud and identity theft. A more secure, trusted solution can be found that meets both the demands of a consumer for frictionless transactions while ensuring an appropriate level of privacy and security. The federal government must create a legal framework to enable the creation and usage of digital ID solutions under one national strategy by leveraging the capabilities of the private sector. Collaboration is crucial to enable Canada's participation in a digital economy both domestically and abroad, spurring innovation and growth while creating a stronger and safer way to manage Canadians' identity.

[i] https://www.finextra.com/blogposting/13903/kyc-and-blockchain

[ii] CBA estimate based on number of Canadians that switched bank accounts from one financial institution to another in the last 3 years according to a CBA survey and the population in Canada 15 years and older as reported by Statistics Canada.

[iii] CBA estimate based on Canadian driver's licence data from University of Michigan Transportation Research Institute, "Recent Changes in the Age Composition of Drivers in 15 Countries" (October 2011) cross-referenced with Statistics Canada, "Estimates of population, by age group and sex for July 1, Canada, provinces and territories" (Table 051-0001 – 2017), and assuming a five-year expiry cycle for driver's licenses.

[iv] TELUS Digital Identity, A Matter of Trust

[v] Equifax, The New Reality of Synthetic ID Fraud, 2015.

[vi] Office of the Auditor General of Ontario, 2015 Annual Report, Chapter 4, Section 4.09, ServiceOntario

[vii] Office of the Auditor General of Ontario, 2017 Annual Report, Volume 2, Chapter 3, Section 3.06, ServiceOntario

[viii] https://id2020.org/digital-identity-1/

[ix] https://www.id.ee/public/The_Estonian_ID_Card_and_Digital_Signature_Concept.pdf

[x] Vassil, Kristjan, Estonian e-Government Ecosystem: Foundation, Application, Outcomes. World Development report, 2016

[xi] http://theconversation.com/what-australia-can-learn-about-e-government-from-estonia-35091

[xii] World Economic Forum, White Paper, Digital Policy Playbook, Approaches to National Digital Governance Report, 2017

[xiii] https://www2.deloitte.com/content/dam/Deloitte/in/Documents/industries/in-india-services-sector-ges-2017-noexp.pdf

[xiv] Maudlin, John. India's Tech Revolution Has Already Left the West Behind –It's the Best Investment Opportunity Now, Forbes

[xv] https://www.businesstoday.in/current/economy-politics/aadhaar-india-government-save-9-billion-cost-nandan-nilekani/story/261996.html

[xvi] World Economic Forum, A Blueprint for Digital Identity, August 2016, p 28