

Digital Identity Innovation – Canada's Opportunity to Lead the World

Digital ID and Authentication Council of Canada Pre-Budget
Submission

August 4, 2017

Canadian governments, banks, telcos, healthcare providers and business of all sizes are vocal in their commitment to becoming more digital – commitment that hinges on Digital Identity.

Digital Identity is a critical, but currently inefficient, layer of the digital era for the safety of Canadians as they continue to do more online domestically and globally. There is no open mechanism for us to control our identity, for trusted third parties to add fragments or attributes to our identity, for us to then carry it around or use that identity around the world and safely interact & authenticate with it.

Current identity tools don't support this modern approach, relying instead on identity documents, processes and methods from the physical world.

Username and password combinations are cumbersome and easily forgotten, while patchwork solutions authenticating users with photos of driver's licenses are less secure and difficult to validate. The result of inefficient identity verification methods is a trade-off between increased cost and risks for businesses and convenience for citizens.

New digital identity standards and tools that are trusted across all areas of the digital ecosystem are required to allow individuals to prove they are who they are, in a secure and privacy-enhancing way. Businesses, governments, and consumers need to combat rising rates of cyberfraud and cybercrime, reduce the risk and friction of transacting digitally, and increase trust and safety for citizens.

Created in 2012, the Digital Identity & Authentication Council of Canada (DIACC) is a neutral non-profit industry led consortium of public and private sector leaders committed to developing a Canadian digital identification and authentication framework to enable Canada's full and secure participation the global digital economy.

DIACC members - including representatives from private sectors leaders as well as the federal and provincial levels of government – participate under the well-established neutral good governance, policies, and tools maintained by the DIACC.

DIACC's objective is to unlock societal and economic opportunities for Canadians by providing the framework to develop a robust, secure, scalable and privacy enhancing digital identification and authentication ecosystem that will decrease costs for governments, consumers, and business while improving service delivery and driving GDP growth.

It's unprecedented that so many Canadian companies large and small and governments have come together agreeing on a common standard and willing to invest their dollars and time in solving a problem so important to all of Canada."

- Joni Brennan, President



DIACC is calling on the government of Canada to seize the opportunity to build a first of its kind digital identity ecosystem through collaboration and investment, which will enable Canada to establish the global standard for digital business and consumer protection. By cultivating user-centric identity solutions, and ensuring the adoption of these tools by leading organizations, we will enhance user security and privacy; incorporate digital identity proofing and authentication processes established by DIACC and the National Institute of Standards and Technology (NIST);¹ lower costs and risks for Canadian businesses and governments to operate digitally; and supercharge Canadian innovation, creating thousands of jobs.

THE BUILDING BLOCKS TO LEAD IN DIGITAL IDENTITY

Leading organizations and institutions have come together under DIACC to develop the rules and tools needed to solve the challenges facing the digital economy. Provincial governments, Canada's largest banks, telcos, credit agencies, and software providers are committed to working together to create world-leading business, legal, and technical standards and solutions to improve identity in the digital age. Supporters of the DIACC Supercluster are laying the foundation for the unparalleled beneficial access, privacy, and security that a digital identity ecosystem provides.

No single group of entities can solve the identity challenge alone. Creating an ecosystem allows companies to leverage the best available information to validate a customer's identity. This technical

implementation of the ecosystem architecture leverages blockchain and distributed ledger technology, which provides the ecosystem foundation. Blockchain facilitates the immutable, secure, and privacy-respecting sharing and validation of digital attributes for consumers and businesses.

Under the proposed digital identity ecosystem, all parties work in a neutral competitive environment to set the business, legal, and technical interoperability standards. The strengths of each organization converge within the ecosystem to create the standards needed to support a world-leading network model enabling privacy, security, and trust in digital identity authentication, verification, and attribute sharing. Standards drive consistent experiences across industries, reinforcing secure user behaviours.

"Canada has a long history of collaboration towards common goals and combining the strength of banking credentials, telco capabilities, credit agencies and government identification will enable a service that increases consumer privacy, security and convenience. The stakeholders involved in this initiative, including Ryerson University, firmly believe that a network approach, in which attribute validation and authentication capabilities are shared, will be more widely adopted and cost effective than each party developing their own proprietary solutions."

– Ann Cavoukian, Ph.D, LL.D. (Hon.), M.S.M – Executive Director,
Privacy and Big Data Institute, Ryerson University



¹ <https://pages.nist.gov/800-63-3/sp800-63-3.html>

SIGNIFICANT BENEFITS FOR ALL PARTIES

Collaboration is necessary to enable the secure digital identities needed for citizens, governments, and businesses in the digital age. Secure, trusted digital identities will allow Canadians to carry out high-value and day-to-day transactions online, in more economically efficient ways without increased risk; will reduce identity theft and improve public safety and confidence by making it more difficult to use identities fraudulently; and will improve healthcare and healthcare outcomes.

Secure digital identities will improve access to government services, regardless of a user's location, that would normally require them to appear in person, and are critical to achieving much of the government's innovation and economic vision - digital identification is inextricably tied to digital economy transformative innovations.

Cost savings regarding password management alone range in the millions. The average administrative cost at call centres to manage and administer lost, forgotten, or stolen passwords is estimated to be \$31 per incident. Assuming one incident per year per working Canadian, across 18.365 million working Canadians, \$570 million is lost annually to just password management services and lost productive hours.²

Improved password management is one of many benefits of a standardized ecosystem. With adequate funding to convene participants, the economic impact on Canada is nearly incalculable. Banks, telcos, and governments stand to save hundreds of millions per year through increased efficiencies. With application to healthcare and patient consent to view and share their records, billions can be saved annually.

In Canada, as the platform grows, it's estimated that 10,000 or more new jobs will be created thanks to new funding and needs.⁴

Case in Point: Accessing Medical Records

A woman from St. Catharines requires surgery at the University Health Network in Toronto. Later, she wants to see her medical records. She cannot verify her identity or access her records online. Instead, she must drive back to Toronto, pay for parking, and show her health card to get a login ID. Once returning home, she hopefully remembers the login and password, along with all the other logins for her local doctor and her medical test facilities. She spends hours trying to access her data and manage her health outcome.

² <http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr66a-eng.htm>

⁴ [Refer to Section C2. Budget and Financial Commitment](#)

With the digital ID ecosystem, data and records could be easily accessed through secure digital ID verification. More convenient processes and systems for individuals and healthcare providers create huge savings in recording and managing consent for research.

While opening new data sources for Canadian health researchers and AI clusters, the secure, simple, and transparent consent management processes developed will save billions in administration costs and time.

A GLOBAL CHALLENGE WHERE CANADA CAN LEAD

Between the business, legal, and technical expertise and commitment of the organizations participating in the DIACC, we can set world-class Canadian standards. Yet digital identity remains a challenge globally – the World Economic Forum identified digital identity as core to evolving the global financial services and FinTech sectors.

Many see a range of European organizations as global leaders in digital identity (e.g., Estonia, Sweden, Luxembourg), spurred by requirements from the EU.

Many of these solutions are based on existing National IDs – a model not applicable to Canada or other geographies. Canadians bring a unique collaborative perspective and thought leadership on privacy, security, and governance. We can provide international leadership, spur job and talent growth, and position our firms as world-leading.



Canada can define world-leading digital identity standards and privacy solutions. This initiative builds on Canada's robust innovation; will increase investment in R&D; boost the economy by mitigating risks, cost savings, and job creation; create companies and growth-oriented firms seeking to participate in the ecosystem; and establish the digital intersection between private, academic, and public sectors.

The future is digital, the future is collaborative, and the future will be realized through a digital identity ecosystem.