2019-07-29

SecureKey Technologies Inc.

Written Submission for the Pre-Budget Consultations in Advance of the 2020 Budget

SECURE KEY

4101 Yonge Street, Suite 501, Toronto, ON | M2P 1N6

Recommendations

- **Recommendation 1:** That the Government of Canada establish a clear policy to allow interoperability of digital identity and data sharing between public and private entities. The policy should be designed to foster the development of a user-centric digital identity and data ecosystem that expands opportunities for economic growth in Canada while protecting the data of citizens, businesses, and governments.

- **Recommendation 2:** That the Government of Canada invest in supporting the growth of a user-centric digital identity and data sharing ecosystem that expands opportunities for economic growth in Canada and fosters an export opportunity for Canadian innovation and expertise at a global scale

2019-07-29

Digital Identity and Data Sharing Networks: An Untapped Opportunity for Canada

About SecureKey

SecureKey Technologies ("SecureKey"), based in Toronto, is a leading Canadian innovator that simplifies consumer access to online services and applications. Using an ecosystem approach and cutting-edge technologies, SecureKey allows consumers to use trusted credential providers -- such as financial institutions and telecom network operators -- to help them connect to critical online services. SecureKey has been the provider of record for the Government of Canada's partner login service since 2012, via a system known as SecureKey Concierge. SecureKey Concierge is currently available for over 80 online services offered by Government of Canada departments and agencies, including the Canada Revenue Agency.

From this base, SecureKey has partnered with seven of Canada's major financial institutions: BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank and TD. This cross-industry consortium of like-minded organizations have worked together to create a holistic, ecosystem-driven solution to digital identity that will better protect citizens, no matter what online services they choose to use.

As a result of this cooperative effort, SecureKey and its partners recently launched Verified.Me – a new, first-of-its-kind Canadian service that helps citizens verify their identities with the digital services of their choice. This next generation technology will allow users to get things done online, in person and on the phone in a safer, more private and risk-reduced manner than traditional security systems. Verified.Me helps confirm identities quickly and securely, using personal information that citizens have explicitly consented to share from their trusted connections.

The Verified.Me service is built upon blockchain technology and is protected with strong security protocols to protect citizens' personal information from being identified, accessed or misused. The service was developed with triple blind™ privacy at its core, meaning that no single party across the service – including SecureKey, as the network operator – can see the complete detail of any single transaction – the destination and source are blind to each other and the network cannot see the data at rest or in motion. Citizens always stay in control by choosing which data, and with whom, to share their information, reducing unnecessary oversharing of personal information in order to access the services they want.

The evolution of digital services

The digital age has ushered in a host of new services, business models and opportunities to participate in the global economy. Not long ago, it would have been unimaginable to order a shared ride from a device in your pocket, or to confidentially access government services from your home. It's not just about citizen expectations. Companies, governments and other organizations have strong incentives to move services and transactions online to enhance client experiences, realize cost savings, and increase business integrity.

Despite the benefits of moving online, the sheer volume of data required to operate the current system exposes vulnerabilities that need to be addressed. The costs and risks to businesses of holding personal data are becoming increasingly evident with each high-profile data breach that occurs. Meanwhile, many consumers do not understand the amount of personal data that they generate when using digital services, nor how that data can be utilized in a variety of ways – good and bad, legal and illegal.

In order to address this challenge, trusted digital identity will be key to enabling the continued development of digital services. From e-commerce to the sharing economy, a robust and reliable digital identity system establishes trust, provides security, and mitigates fraud. As a consequence, we submit that a dependable digital identity system is critical to the development of the Canadian digital economy, and an important consideration for the Committee's work. Ultimately, it is a key tool in making digital services safe, secure, efficient and accessible.

Without it, many of the issues Canadians encounter will be magnified by the rapid increase in digital services and the increasing sophistication and prevalence of online fraudsters.

The Challenge of Digital ID

Today, an organization's ability to operate in a digital environment hinges on a single question…. "Can I trust the person, or digital identity, at the other end of the transaction?"

To recognize clients and provide trusted access to services online, organizations typically deploy a mix of analog and digital measures to confirm identity and mitigate risk. As we have seen, however, these solutions tend to be complex and inadequate -- as a result, confidence in them has suffered.

Typically, citizens are asked to navigate a myriad of identification methods to satisfy the verification requirements of organizations from which they seek services. They do so without knowing where the information is going and how it is being used, and thus with understandable concerns about data breaches and online impersonators. Proving identity has become increasingly difficult – it's inconvenient to do so in person, and fraught with friction in the digital world, where the risk of fraud and identity theft is higher. Fraudsters are collecting information to know as much -- and sometimes more -- than the citizens they are impersonating. Standard physical cards are easily counterfeited, and it is often impossible to check their validity with the issuing sources at the time of transaction. Even biometric methods like fingerprints, which have often been touted as the solution to digital fraud, are targeted by hackers, increasing the risk that biometric data may be compromised.

These factors are driving complexity up, trust in the system down, and adversely affecting privacy -- exactly the opposite of what needs to happen. Our siloed system of identity proofing is too hard for consumers to use and too expensive to be sustained. Collectively, we then need to address the challenge, and reap the opportunities of digital identity.

The opportunity of Digital ID

Conservative estimates peg the potential value of trusted digital identity to the Canadian economy at roughly 1% of GDP, or $15 billion[i]. An even more optimistic outlook suggests "there is 3-6% economic value by 2030 from the good use of digital ID".[ii] In fact, right across the economy, identity is key to delivering services and the benefits are especially evident in several sectors.

The need for digital identity today is seen most immediately in regulated services, such as financial services where companies are required to perform rigorous "know your customer" checks on users at account opening and periodically thereafter. These checks are an important part of helping to prevent money laundering and funding of terrorism, but they are also time-consuming, costly and often redundant. In Canada, research has identified potential net savings per institution at or above $100 million per year through operational efficiencies created by reducing manual processing costs and reducing fraud. [iii]

Trusted digital identity is also needed for a wide variety of online retail and commercial scenarios where payment is required between two parties. This is especially true when there is no prior relationship between the parties, and there needs to be some ability to reduce the risk of fraudsters. Payments in a digital environment require a significant amount of trust since you cannot "see" the person on the other end of the transaction and there is often no straightforward way to digitally verify an authentic person or organization.

Solving the Challenge of Digital ID

The challenge we face is not simply a matter of finding the best technology, the right skills, or enough money to fix the problem; rather, everyone with a stake in the system needs to focus on solving the digital identity problem that underpins all digital services. We need to ensure data and identity information are under the control of the citizen.

Experience to date proves that single factor methods are not up to the task. This means that trusted networks – 'ecosystems' of trustworthy participants -- are needed. All participants must be involved in the solution, especially citizens, whose control over their own data and privacy will underpin its security.

Only by combining the best strengths of each ecosystem player can we solve the digital identity problem and rebuild the trust that is equally required by both organizations and citizens. Imagine a scenario where a citizen can choose to share information securely within a network made up of organizations that they already trust and have ongoing transactions with. Using this layered approach to proving identity, we get a significantly higher level of confidence in the identity of the person conducting the transactions. The challenge is how to do this without becoming a surveillance network or creating a 'honey-pot' of data. In short, we need to establish the basis for privacy and trust while minimizing the volume of data being shared between parties.

The best means of verifying identity and establishing and maintaining trust is to leverage multiple, verifiable sources of information which can be combined to provide much higher identity assurance. A successful network like Verified.Me will bring together these factors from multiple providers, for instance a collaboration of financial institutions, telecommunications providers, and provincial governments to ensure robustness. Such a system can rely on three factors: 'what I know' (something only the individual has knowledge of such as a secure password); 'what I have' (a unique item such as chip card or mobile phone); and 'what I am' (such as a biometric identifier or facial scan). For example, a person using a device that their telecommunications provider recognizes, is logged in to receive services with their bank, sharing information that comes directly from authoritative sources (e.g. government) with the information from the provider (e.g. bank) matched and validated against each other. This creates a secure and seamless experience for the user.

Public-Private Cooperation is Required

While the benefits of an ecosystem approach to digital identity are recognized, no single organization or company can solve the challenge on their own. All parts of the digital economy rely on digital identity – which means there are many potential stakeholders and differing needs. At the same time, the urgent need to put consumers in control of their digital identities mean that it is no longer good enough for each stakeholder to go in their own direction. Organizations of all types, both in the public and private sectors, need to collaborate in the establishment of standards and in the creation of a robust ecosystem that serves everyone's interests.

Examining global best practices, the most successful systems span the public and private sectors and involve substantial coordination between highly regulated sectors and government. Successful examples include NemID in Denmark and BankID in Sweden where users take advantage of high velocity banking credentials for lower regularity interactions with things like healthcare and government. In contrast, systems which have been designed in isolation have been plagued with issues and are not practical models for Canada to follow. These include UK Verify - which has been challenged by low uptake and a high implementation cost – and Estonia ID which employs a centralized government issued unique national digital ID and chip enabled identity card, a model not contemplated in Canada.

With a system of well-regulated core industries and a collaborative public-private environment, Canada has an opportunity to solve the digital identity challenge and establish itself as a model for the world. By demonstrating cooperation between jurisdictions, deploying technologically advanced telecommunications, and supporting and embracing new approaches, Canada can be a world leader, effectively setting the standard for digital identity. We are already recognized internationally for leading ideas such as Dr. Ann Cavoukian's Global Privacy and Security by Design initiative, and the Pan Canadian Trust Framework which has been championed by the Digital Identity and Authentication Council of Canada.

The cyber risk around digital identity is high, but we can build services that can provide identity validation claims from multiple parties in a single transaction, while ensuring complete privacy and control for the citizen. The responsibility to protect privacy and to provide a sense of security to citizens are fundamental factors in the success of any solution.

It is critical that Canada's approach connects the trusted parts of the digital economy such as finance, telecommunications, government, and commerce. Ultimately, any solution that does not involve both the private and public sectors will be of limited success as it would perpetuate the siloed approach that is currently under strain.

Contact

Eric Swedersky, SVP, Delivery and Public Sector
Eric.Swedersky@securekey.com

---

[i] The Economic Impact of Digital Identity in Canada. The Digital ID & Authentication Council of Canada. 2018.
[ii] Digital Identification: The Key to Inclusive Growth. McKinsey and Co. 2019
[iii] The Economic Impact of Digital Identity in Canada. The Digital ID & Authentication Council of Canada. 2018.