Peace of mind in the digital age?
It's possible!

Foreword

In this paper, several private companies serving millions of individuals and businesses in Canada present a shared vision of digital identity and how it fits into everyday life. The goal is to develop a common understanding of digital identity (digital ID), answer basic questions that citizens, consumers, and business leaders may have, foster collaboration among the stakeholders involved in implementing digital ID, and help create an environment conducive to adopting digital ID in Canada.

This paper is the result of the collaborative efforts of Beneva, Desjardins Group, KPMG, TELUS and Videotron, with the support of IDLab, a non-profit organization committed to better cybersecurity through secure and user-friendly digital identities. This white paper on digital ID is being released free of charge by the endorser organizations below.

Table of contents

Summary

- Companies and governments worldwide are increasingly using new digital processes and mechanisms to verify identity.

- However, statistics show that the parties involved still need to gain their users' trust.

- The lack of a truly digital ID further exposes Individuals and organizations to fraud, identity theft and other forms of cybercrime.

- Accessing online services currently requires using "identifiers" such as JDOE and "authenticators" like passwords.

- Because identifier-authenticator combinations are difficult to manage, personal information ends up being collected and dispersed into the digital space.

- A digital ID is not a unique identifier, but rather a set of verifiable credentials specific to a person (birth certificate, driver's licence, membership card) stored in a person's digital wallet. The individual has full control over these credentials.

- Digital ID places the individual at its core and is based on three pillars: agency, autonomy and information integrity.

- Digital ID also discourages fraud, because there's no longer a "vault" containing information on millions of people. Instead, these same people hold and control their personal information.

- Digital ID will make people's lives easier, give them more control over their personal information, improve their security and sense of safety, and benefit the economy by reducing fraud-related losses.

- Most countries are moving toward digital ID. It will be implemented in tandem with governments, businesses and the public. Digital ID is a necessary evolution for society.

Background

In our everyday lives, we need to identify ourselves to access many services. And each time, the organization we are contacting must be able to verify our identity.

Whether you're obtaining government services—education, health care, permits—or dealing with a financial institution, a telecommunications service provider, or an insurance company, you first have to identify yourself and prove that you are who you say you are.

The identification and authentication process is a cornerstone of our economic and civic life. However, this process is long, complicated and can be flawed.

A 2019 study by McKinsey[1] found that implementing a digital ID process would add, by 2030, 3% to 13% to the GDP in the seven countries studied (Brazil, China, Ethiopia, India, Nigeria, the United Kingdom and the United States).

More and more companies and countries worldwide are using new identity verification processes, technologies and mechanisms. The benefits of an identification and authentication process using a provincial, national or even international digital ID are undeniable. Digital ID offers a better user experience that's streamlined and accessible, reduces fraud risk and lowers management costs.

However, statistics show that the general public and other stakeholders don't always trust these suggested solutions, which prevents them from being adopted. There are many reasons for this:

- Inherent risks in the digital technologies we're already using.

- Recurring incidents of personal information being hacked and identity stolen.

- Concerns about who controls and uses personal information and its traceability may lead to an invasion of people's privacy.

As soon as we learn more about the topic, we quickly note that the current state carries far more risk. The lack of an official digital ID further exposes people and organizations to fraud, identity theft, and other forms of cybercrime.

We must educate people and raise awareness about digital citizenship in order to garner broad support for digital ID. Only then will we be able to create the best possible conditions to achieve this desirable and inevitable evolution of the way we enter into relationships with public and private organizations.

This document plays a part in that.

---

[1] McKinsey, Digital identification: A key to inclusive growth, April 2019.

What is "digital identity"?

At its core, a digital ID is a digital representation of a person that proves their identity allowing them to interact with organizations and access services easily and securely. Let's look at the limitations of the current state to fully understand digital ID and its benefits.

The limits of "identifiers" and "authenticators"

Every day in our digital life, we use "identifiers" and "authenticators." An identifier is a user name such as JDOE, for example. It is a way for an organization to uniquely identify an individual. The password linked to it is the authenticator. You can share your identifier so people can contact you, but only you should know the combination of identifier and password that you use for interactions such as accessing your bank account, filing your tax return, making online purchases, etc.

Managing our identifiers and authenticators can be challenging: we usually have many of them, each with a complex password that includes numbers, letters, capital letters, symbols, etc. However, users do not always have the knowledge and discipline, nor are they diligent in managing all their authenticators appropriately. What's more, the use of authenticators makes it difficult or even impossible for an organization to be sure that the person really exists and that they are indeed who they claim to be.

This lack of trust or certainty limits what we can do online.

More and more organizations are using two-factor authentication to mitigate these risks. For example, a person who logs into a transactional site may identify themselves as JDOE, authenticate that identifier with their password, and then authenticate a second time using a code they received via text message. This is certainly an additional layer of security, but the operation can be time-consuming, and it still doesn't provide the security that a proper digital ID can.

In reality, our online identity is split into countless identifiers and authenticators that could each be used as part of a security breach.
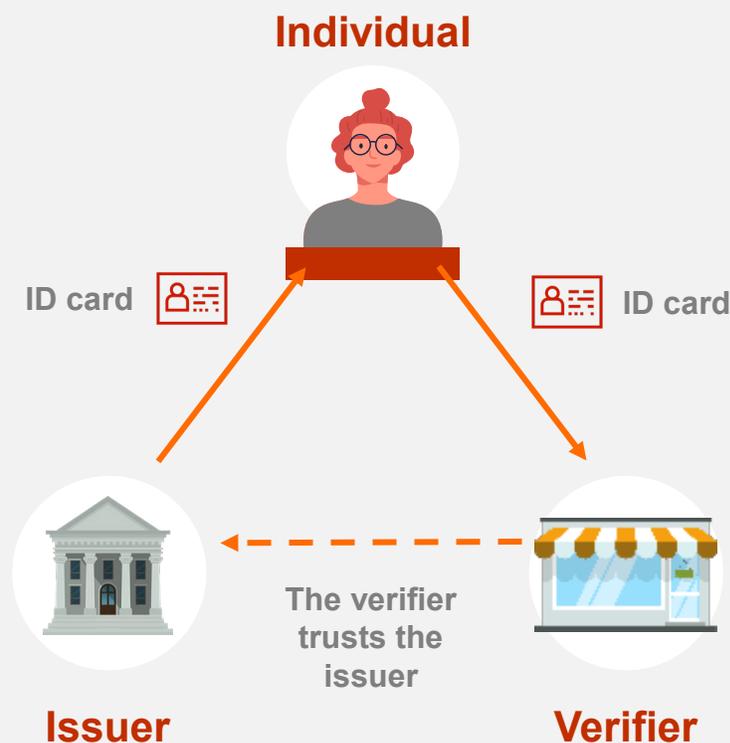
What is "digital identity"?

The physical world's trust triangle

In the physical world, when you have to prove your identity, you're asked to provide a document with photo ID like your driver's licence, health insurance card or passport. These forms of identification are recognized because credible sources, like governments, issue them and because they have security features to prevent counterfeiting. People generally trust these documents.

In the physical world, a **trust triangle** exists among a credible issuer that gives a real person an ID card that the verifier (a public or private organization) will accept as valid because it trusts the issuer.

Digital ID aims to recreate a trust triangle in the digital space. This requires the ability to provide identifying information using digital documents that can be verified for their accuracy and authenticity and are issued by trusted organizations.

**FIGURE 1.**

The Trust Triangle in <u>the Physical World</u>

Individual

ID card

ID card

The verifier trusts the issuer

Issuer

Verifier

What is "digital identity"?

Recreating the trust triangle in the digital world

The same relationship between the issuer, individual and verifier must exist to recreate the **trust triangle** in the digital world.

Stakeholders have to follow conventions, standards and regulations, but have the support of new tools for their interactions, such as verifiable credentials, the digital wallet and a verifiable data registry.

FIGURE 2.

The Trust Triangle in the Digital World

Individual

Verifiable credential

Digital wallet

Verifiable credential

Trust

Verifiable data registry

Trust
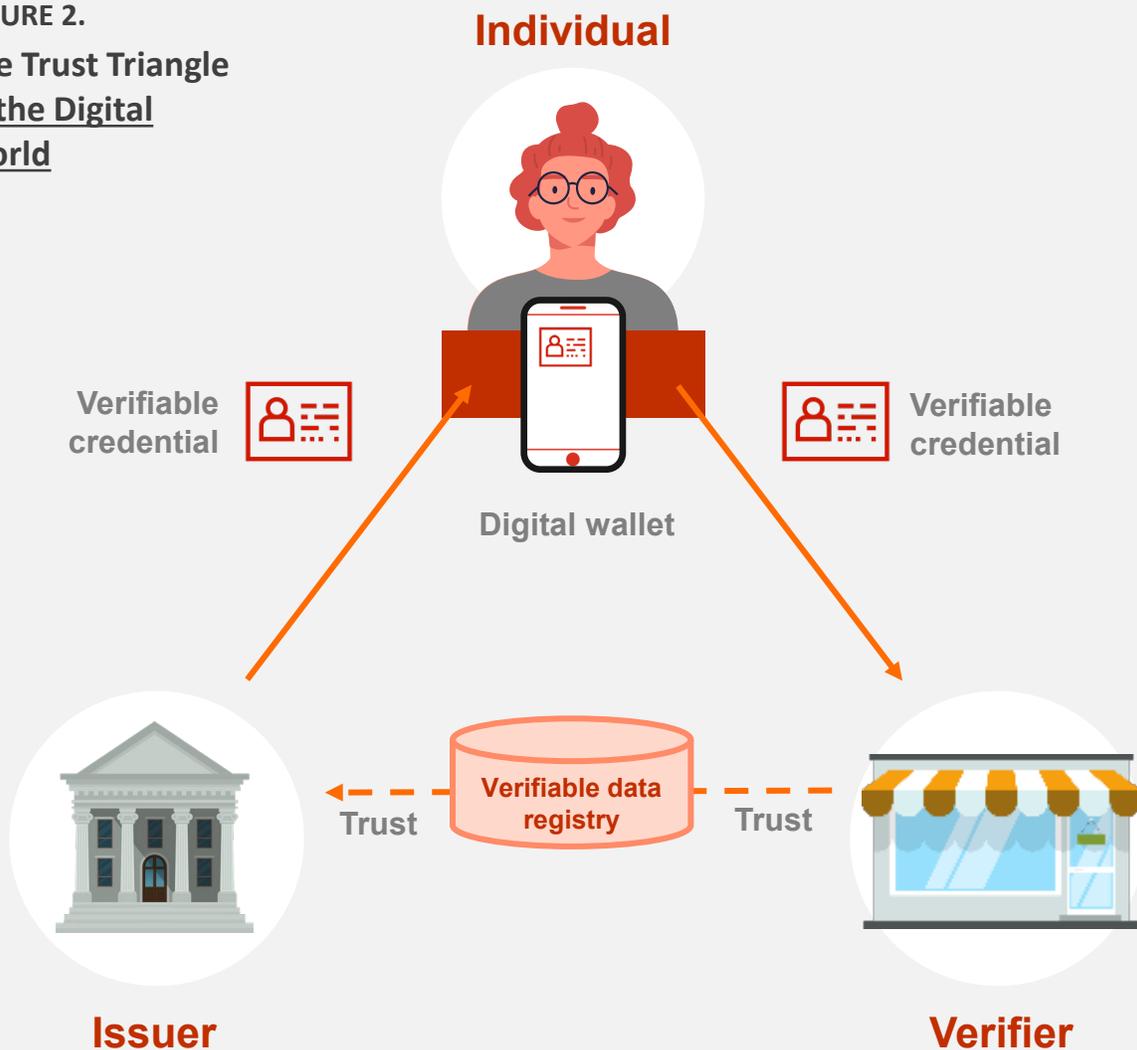
Issuer

Verifier

What is "digital identity"?

Recreating the trust triangle in the digital world (cont'd)

Verifiable credentials (issued)

These are digital documents that the issuer has signed electronically. This ensures that the verifier who receives information from a verifiable credential can always verify its authenticity and integrity, which increases the level of trust in comparison to physical documents. These credentials are added to a digital wallet held by an individual. That way, the person controls their information because they are the owner and must consent to sharing their data with a verifier.

Digital wallet

This is typically an app installed on a smartphone. It serves as a secure repository for verifiable credentials and makes digital interactions possible.

Verifiable credentials (presented)

An individual can present their verifiable credentials to a verifier without giving all their data. For example, if a verifier wants your first and last name, there's no need to provide other personal information, like your date of birth. Similarly, you can prove that you're old enough to buy alcohol without necessarily sharing your date of birth.

Verifiable data registry

A verifiable data registry is used to verify that a trusted issuer has issued a credential and has not revoked it. The verifiable data registry does not store any personal information.

Digital ID is, therefore, not a unique identifier like a digital SIN, but rather a set of verifiable credentials specific to a person (birth certificate, driver's licence, membership card) contained in a person's digital wallet and under the sole control of that person.

How is digital identity a step forward?

Today, all of our digital interactions leave a trail. They are our digital footprints, which can be found throughout the digital space. When we shop online, post a comment on social media, or read an ad on a website, we leave a trail that can identify us either directly or indirectly.

Strengthening privacy protection

But beyond the digital trails we leave behind every day, we must realize that we share much more personal information than we need to most of the time. For example, we should only show our driver's licence to authorized government officers, yet we show it in all kinds of situations. We show it when we go to a hotel, the library, and the liquor store. It's all too common. We also create user accounts for all our Internet subscriptions: e-commerce websites, social networks, and information sites. We agree to share a lot of personal information for each of these accounts, including our first and last name, address, date of birth, telephone number, and much more.

Our personal information circulates broadly, and its protection depends on the security measures put in place by the organizations that collect and store it. Despite increasingly strict laws, the quality of organizations' security processes varies widely.

The information needed to access a person's user accounts or even to fraudulently create accounts in someone else's name is sometimes very easy for an ill-intentioned third party to obtain.

How is digital identity a step forward?

Strengthening privacy protection (cont'd)

Governments are cracking down with harsher penalties for mismanaging personal information. But this punitive approach doesn't address the core issue: storing and sharing personal information online has become non-secure and obsolete.

The movement toward digital ID is global. Both governments and private organizations are advocating for it. Although digital ID models are still in development and differ from one another, they are all intended to give people control over their personal information so that they only share it with trusted third parties who have obtained their formal consent.

Canada is no exception, and the various public and private stakeholders are working together to implement means of identification that improve the protection of personal information and people's privacy.

Building digital trust

One of the most significant gains from digital ID is people's control over their personal information. In today's world, we must constantly prove who we are. That usually requires that we provide photo identification from a government or trusted institution, which forces us to share far more personal information than necessary. This practice, while unavoidable, is not safe for the individual. Personal information is also a sensitive asset for the organizations that become the custodians of this information and must do more and more work to ensure it's protected. The current situation poses risks for everyone involved.

For digital ID to be a solution, it must be based on mutual trust. **The notion of trust is vital to the work being done to implement digital ID.**

The public and private sectors are working together to develop trust frameworks to guide digital interactions and lay the foundation for digital trust in Canada.

Personal information breaches and cyberattacks have intensified in recent years, and identity fraud has followed the same trend. Collectively, we have come to the point where we must reinvent the way we identify ourselves, in both the digital and physical worlds. The way forward is to introduce digital identities.

How is digital identity a step forward?

Building digital trust (cont'd)

Globally, all eyes are on the two Pan-Canadian Trust Framework models: the Government of Canada[2] model that focuses on public organizations and the Digital Identity and Authentication Council of Canada (DIACC) model[3] that stems from a coalition of public and private sector leaders.

These models also aim to steer the standardization of national and international digital ID ecosystems by applying the required policies, standards and technologies. In addition to this work, government authorities and some certification bodies are preparing a regulatory framework and certification standards that the various stakeholders in the digital ID ecosystem must comply with to be considered trusted issuers. In this way, the digital credentials they issue can be trusted by other ecosystem members.

Digital trust is only possible if there's a national consensus on trust frameworks, more commonly referred to as governance frameworks, like those developed in Canada, and only if the government bodies give them the legitimacy they need by putting in place appropriate standards and regulations. Pillars and operating principles will make it possible to achieve this alignment.

---

[2] CIO Strategy Council, Digital Trust & Identity – Part 1, Sept. 2020.

[3] DIACC, Pan-Canadian Trust Framework Overview, 2021.

These trust frameworks, as described by DIACC, are "a set of rules and tools designed to help businesses and governments to develop tools and services that enable information to be verified regarding a specific transaction or particular set of transactions."

Digital identity pillars and principles

We believe that digital ID must be people-centric to gain strong (voluntary) buy-in. It must first reinforce the idea of the individual. Each person must feel in control of their information. It's this fundamental assurance that will ensure that digital ID will also be beneficial for society as a whole and for the economy.

However, digital ID is not just for individuals. Companies will also have digital ID. The real challenge is ensuring the solution are human centric. Following the work of several experts[4,5], these guiding principles were written.

These principles show us how we can put in place a trusted digital ID ecosystem that meets everyone's needs and expectations.

The principles fall under three pillars: **agency, autonomy** and **integrity.**

---

[4] Sovrin, Principles of SSI v3, September 2022. We've adapted the descriptions of the principles to make them easier to read and understand.

[5] Drummond Reed and Alex Preukschat, Self-sovereign Identity, May 2021.

Digital identity pillars and principles

Pillars	Principles
Agency "Every human being is in control and has agency over their personal information and identity."	• Being able to choose the credentials you add to your digital wallet to represent yourself: your municipal library card, driver's licence, passport, etc. These credentials are different ways to represent yourself, depending on the context. • You may also choose, for any reason, to delegate your credentials to someone that you choose (agent) or, should you become incapacitated, you can plan to give power of attorney to a third party. • You will have access to every service and privilege, with no discrimination. Equality and inclusion will be promoted. • You will benefit from an optimal user experience through the features offered to you.
Autonomy "Every human being has the right to freedom of choice and no constraints on the management of their digital identity."	• You can choose to participate or not in the trusted ecosystem that will be put in place for digital ID. • You can make sure that your personal information is not tied to any single organization, and you prefer that other organizations be able to verify it independently. • You can interact with many services, individuals and organizations in a completely transparent way. With your consent, systems are able to communicate and exchange information without you being impacted. • You can securely move or transfer a copy of all your credentials to another digital wallet without worry or commitment.
Integrity "Every human being has the right to protect and safeguard their personal information."	• Your information is secure, and you always have control of your credentials. • You can provide verifiable proof of the authenticity of your personal information. • You can keep your personal information confidential and share the minimum data with anyone who asks. For example, proving that you are 18 or older without revealing your actual date of birth. • You can easily access all the rules, policies and processes that govern the digital ID system with which you interact.

Digital identity in everyday life

Digital ID will be part of everyday life. It will be easy to use, secure and will allow everyone wishing to use it to have control over their personal information. This information will only be shared with the individual's consent, and each time, only the minimum required information to obtain the service will be shared. Digital ID will end the spread of personal information.
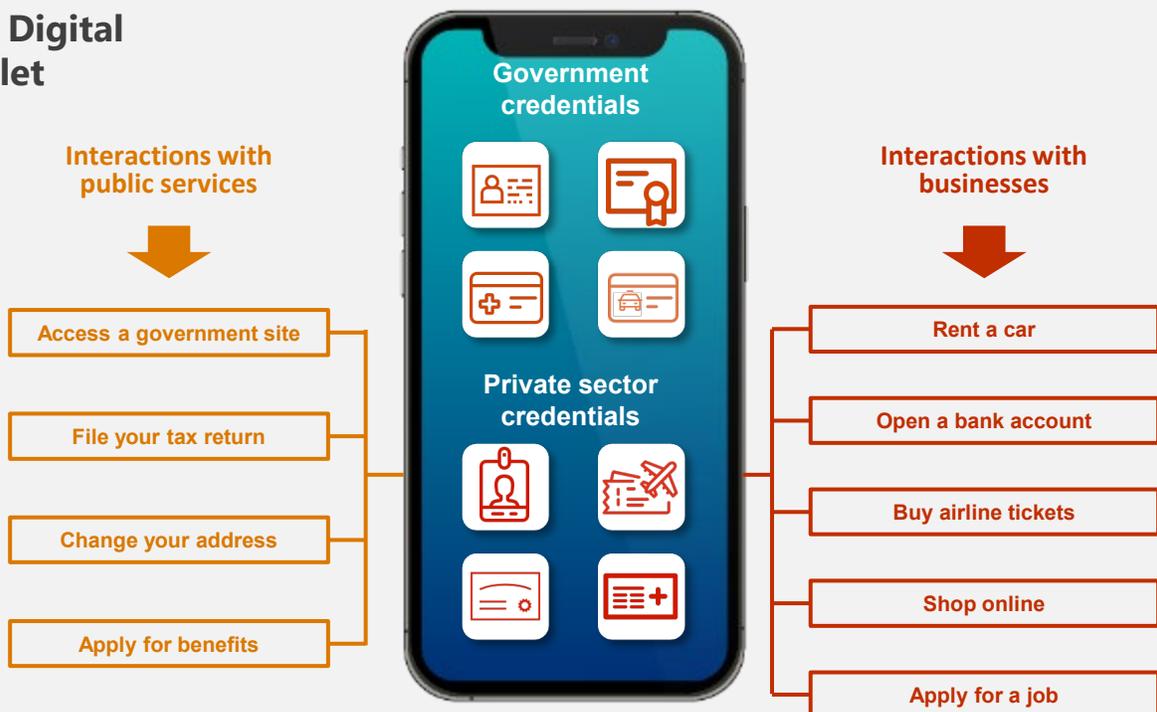
The combination of a digital wallet and verifiable credentials will open the door to a wide range of uses affecting both private life (leisure, spending) and interactions with public services.

For example, suppose you need to rent a car. You could do it online by providing the rental company with your relevant personal information, driver's licence and proof of insurance from three different issuers. The rental company would be able to verify the integrity and authenticity of the information.

People who don't have smart devices or would not want to use digital ID could continue to access services using the current traditional means.

In the next section, we'll describe a few real-world situations.

FIGURE 3.
The Digital Wallet

Interactions with public services

Government credentials

Interactions with businesses

Access a government site

File your tax return

Change your address

Apply for benefits

Private sector credentials

Rent a car

Open a bank account

Buy airline tickets

Shop online

Apply for a job

User journey
Getting a new job

Step 1: Apply for a job

Taylor has just graduated and hopes to work for a well-known digital marketing company. To apply, the company asks Taylor to provide proof of an undergraduate degree before continuing the process. Taylor uses the educational credentials issued by the university that have been saved in their digital wallet to complete the application.
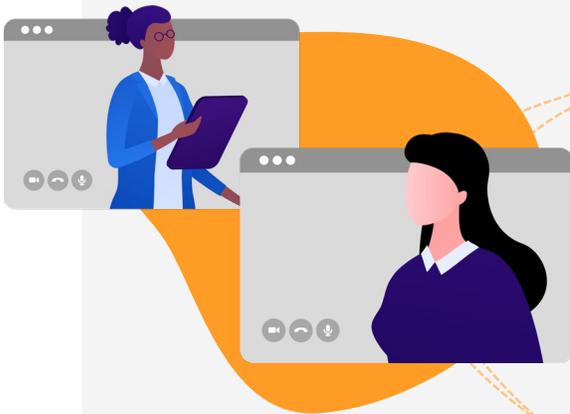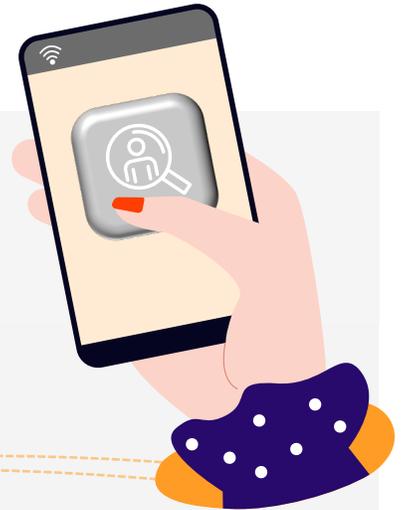
Step 2: Interview and job offer

Taylor meets the requirements and has a virtual interview. A few days later, the employer sends a job offer outlining the new role, salary, bonus structure and benefits. Ecstatic about the news, Taylor uses their electronic signature to accept the offer!

Step 3: Information sharing

Taylor must provide several pieces of information so that the company can create an employee file and pay their salary via direct deposit every two weeks. Taylor uses their digital wallet to select only the verifiable credentials required by the company, providing a detailed view of the requested information.

The company confirms the authenticity of the verifiable credentials received, completes the file opening and issues a credential stating Taylor's role and salary.
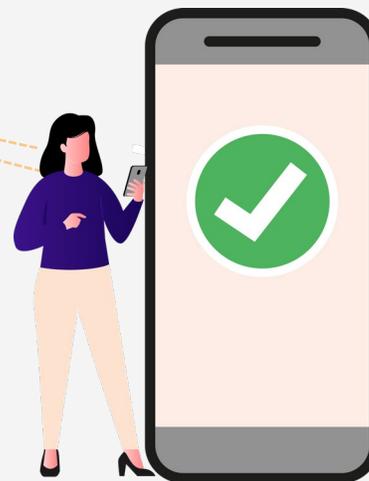
Examples of verifiable credentials:
- **Banking information**
- **Identity (SIN, age, nationality, etc.)**
- **Address**
- **Work permit**

Step 4: Additional information

A few months later, Taylor's employer issues tax slips, which Taylor adds to their digital wallet in order to eventually share them with the provincial and federal governments. Taylor knows that the personal information shared with the employer can be revoked if the employment ends.

User journey
Opening a new bank account[6]

Step 1: Open a bank account

After landing their new role, Taylor opens a bank account through their financial institution's app.

Step 2: Information sharing

The app asks Taylor if they want to use their digital wallet to confirm their identity. It lets them select only the verifiable credentials the financial institution requires and then shares them securely.

Examples of verifiable credentials:
- **Proof of employment**
- **Identity (SIN, age, nationality, etc.)**
- **Proof of residence**

Step 2: Validation and approval

The financial institution confirms the authenticity of the verifiable credentials it received and processes Taylor's application. Thanks to this efficient process, Taylor quickly receives an email confirming their new account with the financial institution.
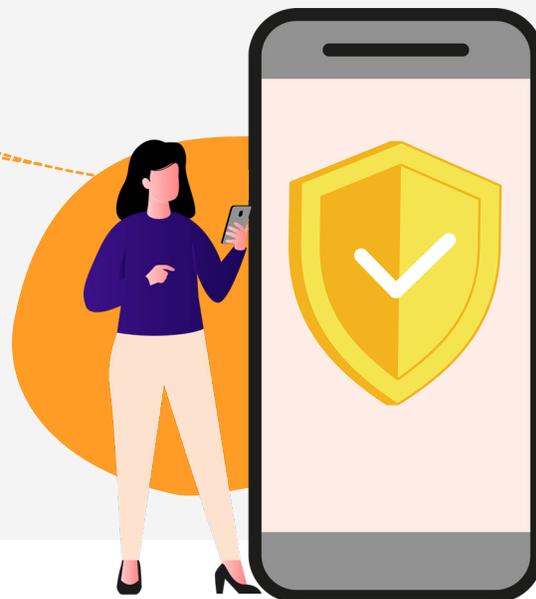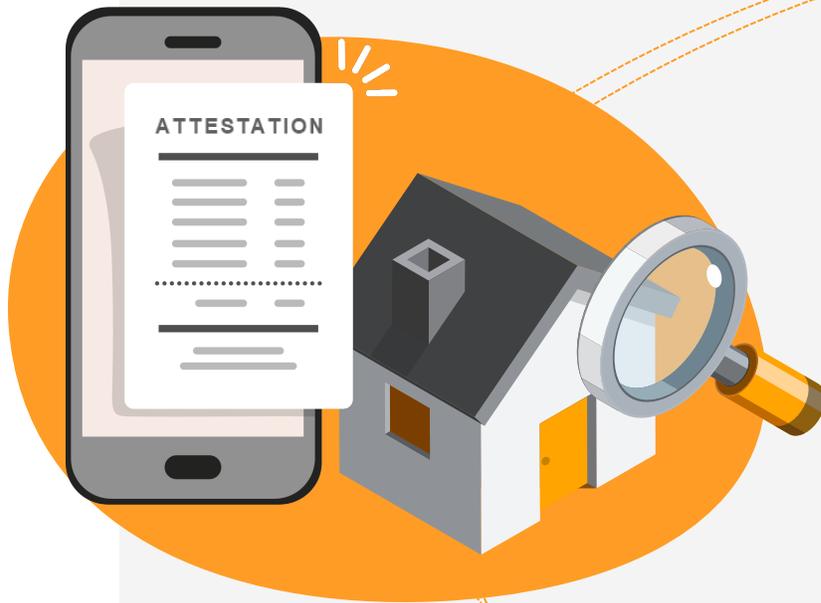
[6] Ontario, Ontario's Digital ID: Where it could be used, June 2022.

User journey
Applying for a mortgage loan[7]

**Step 1:** **Loan application**

After a few years in their new role, Taylor gets promoted and wants to take out a mortgage loan to buy a home. Their application is submitted through a mobile app accessible via their digital wallet.

However, their application requires additional verifiable credentials confirming the answers Taylor provided in the loan application about income. Taylor quickly shares the information with the financial institution via the app by using the employment credentials provided by their employer and stored in their digital wallet.

Step 2: **Validation and approval**

The financial institution confirms the authenticity of the verifiable credentials it received and processes Taylor's application. The loan is granted after approval.
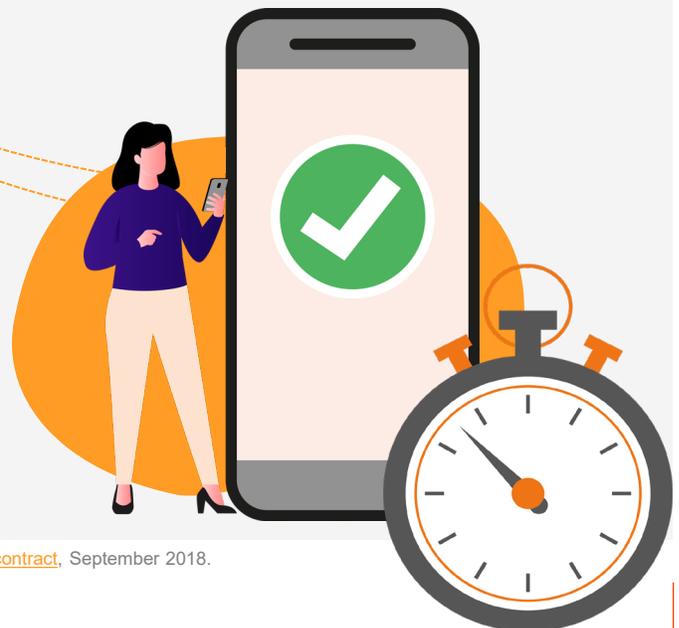
[7] World Economic Forum, _Identity in a Digital World A new chapter in the social contract_, September 2018.

User journey
Traveling by plane

Step 1: Check-in

After planning a ski trip to British Columbia, Taylor arrives at the airport, checks their baggage and heads to security. Taylor opens their digital wallet, preparing their digital travel credentials for verification.

Examples of verifiable credentials:
- Digital ID or passport
- Boarding pass
- Public health attestation (e.g. COVID-19)
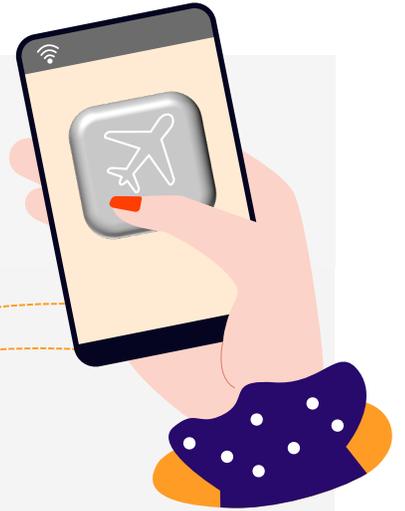
Step 2: Identity verification

At this stage, Taylor must share the information using their digital wallet. The terminal flashes green once their identity has been verified. After verification, the information exchange is logged in Taylor's digital wallet, and they continue on their trip.

Step 3: Car rental

While waiting for their flight, Taylor reserves a car in British Colombia. The rental company requests Taylor's consent to access their verifiable credentials. Taylor uses their digital wallet to select only the verifiable credentials required to fill out the rental form.

Examples of verifiable credentials:
- Identity (interprovincial with minimal disclosure of age)
- Proof of insurance
- Driver's licence

Step 4: Validation and approval

The verifiable credentials are quickly authenticated and the company asks Taylor to e-sign the contract. Once in British Colombia, Taylor picks up the keys at the counter and leaves the airport.

What are the benefits of digital identity?[8]

Improved security and privacy of personal information

- Better security and protection against identity theft, information leaks and fraud primarily because data is decentralized.
- Data is protected with a high level of security, and unlike your physical wallet, your digital ID can easily be turned off if your phone is lost or stolen.
- Privacy : Less personal information gets collected and stored by organizations.

Better control over your personal information

- More informed consent: you only disclose the required information at a specific time.
- Full control over what you want to share and with whom.
- No one can access your personal information without your consent.
- Reduced need to manage multiple identifiers and passwords and less potential for error.

Better services

- More public and private services are available digitally, which means less time spent waiting in line.
- Access to new services that were previously unavailable or unknown.
- Overall improvement in the online customer experience.
- Convenient—digital ID is stored on your mobile device and is always ready to use whenever you need it.

[8] McKinsey, Digital identification: A key to inclusive growth, April 2019. BC Government, BCeID Authentication Service, 2022.

The fight against fraud

With vast amounts of personal information in circulation, our current state presents risks that we can attempt to mitigate with good password habits and two-factor authentication processes, for example. Incidents of fraud, privacy breaches, and theft of personal information are one the rise, despite our best efforts, investments, and increased user awareness. One of the clear benefits of digital ID is its ability to fight fraud more effectively. Let's see why.

You could say that a fraud economy boils down to this: before acting, a fraudster weighs the cost of committing fraud against the potential gains. Fraud is worth the effort if the profits outweigh the costs.

Digital ID changes the cost-benefit ratio of fraud, because an individual's personal information is stored as verifiable credentials in their own digital wallet rather than in a centralized database.

As a result, only the person holding the verifiable credentials can prove that they control their digital wallet. For a fraudster in Canada, this means that 38 million digital wallets would need to be defrauded to get the same result as hacking into a single centralized database. Furthermore, having personal information will no longer be enough. The fraudster will also have to prove that the verifiable credentials were issued to them.

Today, a fraudster with another person's social insurance number can successfully impersonate them to fraudulently obtain services or benefits.

With digital ID, having someone else's social insurance number is not enough. You have to prove that the information is yours. This is possible through the encryption used to create the verifiable credentials that you'll have in your digital wallet.

The fight against fraud

Simply put, a social insurance number with more digits or security features that exist is unnecessary. We can continue to use our existing information to identify ourselves, use services, or prove all sorts of things about us. But it will require creating verifiable credentials based on our existing official information or documents.

In short, our verifiable social insurance credential will be cryptographic proof of our current social insurance number that Service Canada will create.

Digital ID renders stealing personal information unappealing and no longer financially rewarding to fraudsters.

What it will take to implement a digital identity ecosystem

Here are some of the winning conditions that promote trust and buy-in from the largest number of people, public organizations, and private companies to deliver the expected gains from digital ID:

Implementing **robust** and **effective governance** in the form of legislation, policies, regulations, roles, responsibilities and processes within digital ID ecosystems.

Buy-in and support from **public and private sector organizations**.

Adhering to operating principles that put people at the centre of the system based on the pillars of Agency, Autonomy and Integrity.

Role of private organizations

Digital ID relies on a collaborative ecosystem built on mutual trust. This ecosystem comprises many public and private organizations, each of which will have a pivotal role to play in their respective sectors. Every stakeholder must trust the processes and rules that will be implemented.

What would be the role of private organizations? Three key words: contribution, trust and adoption.

Contribution

As issuers and verifiers of credentials, private sector organizations will play a substantive role in developing and growing the digital ID ecosystem. Private companies are key partners in building a solid ecosystem, leveraging their vital presence in people's economic and social lives, investment capacity, innovation and technological know-how. It's through their ongoing involvement that we can build trust.

Trust

The contribution of the private sector and collaboration between the government and the private sector will underpin the trust that the digital ID system can instill in the public. Depending on the circumstances, companies will be trusted verifiers and issuers in the digital ID ecosystem.

By working in partnership with the public sector, we will be able to provide support and expertise to governments to ensure that the implemented solutions meet the needs of both the public and private sectors. This will help create a strong relationship based on trust to promote adoption.

Adoption

Private companies will contribute to developing digital ID in collaboration with the government, which will build public trust and foster widespread adoption of digital ID by citizens. Moreover, since the private sector accounts for about 65%[9] of Canada's jobs and GDP, businesses will be the primary entry point for digital ID into Canadians' lives. Businesses will have to be ready to make the transition. They will have to inform and educate their clients. They will also have to provide support. Businesses will play a key role in developing a user-friendly digital ID experience.

[9] Institut de la statistique du Québec, Bilan du marché du travail au Québec en 2022 (quebec.ca), March 2023.
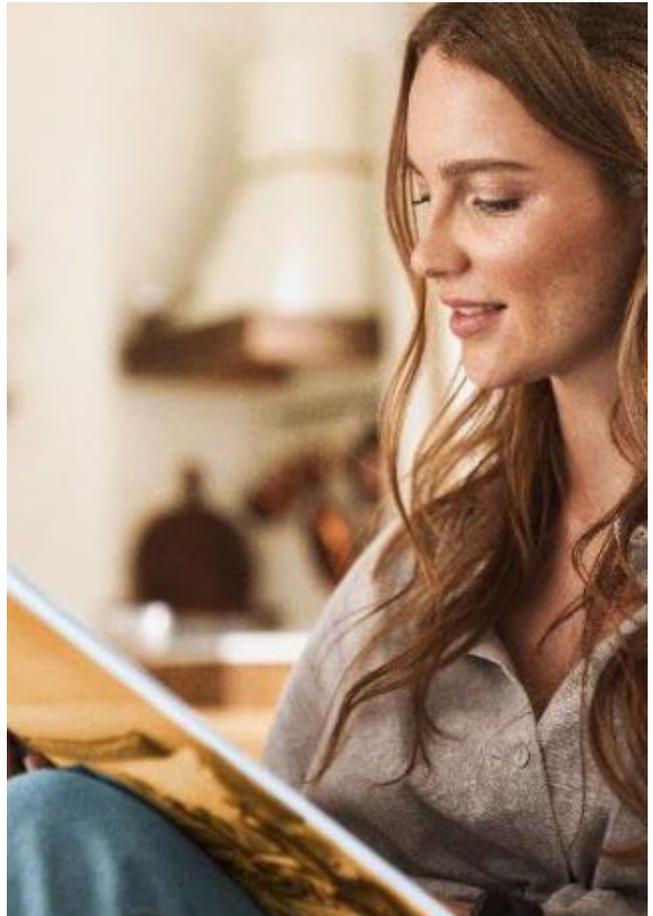
Digital identity here and abroad

The Government of Canada's vision[10] is to create a digital ID ecosystem where trusted digital ID is used to provide Canadian government services transparently on any platform, with any partner, and on any device.

Digital ID is a global trend

The **World Bank** estimates that "as many as 1 billion people across the world do not have basic proof of identity, which is essential for protecting their rights and enabling access to services and opportunities[11]" (e.g. education, health care and employment).

At the **United Nations**, increasing awareness of the need for more inclusive and robust identification systems has led to a global call to action, as seen in target 16.9 of their Sustainable Development Goals: "By 2030, provide legal identity for all, including birth registration.[12]"

---

[10] Canada's trusted digital identity vision.

[11] World Bank, Principles on Identification for Sustainable Development Toward the Digital Age.

[12] United Nations, Sustainable Development Goal 16.9.

Digital identity here and abroad

Digital ID is a global trend (cont'd)

The importance of involving every stakeholder in the ecosystem and having verifiable credentials that can be used across Canadian jurisdictions and internationally will require a widespread collaborative effort. The provinces, the territories and the federal government will have to work together and with industries and other countries to explore opportunities to extend credential recognition to the private sector, across provinces and even outside the country. Alberta and British Columbia, for example, have conducted preliminary reviews of their digital ID credentials to ensure that the federal government accepts them.

Here are a few examples of Canada's involvement in international initiatives:

- Canada and the European Union (EU) are working on ways of recognizing the use of digital credentials—including transactions conducted through digital wallets—for business and personal use.

- Canada is one of eight countries that created a digital ID working group in 2020. The group, chaired by Australia's Digital Transformation Agency, includes Australia, Finland, Israel, New Zealand, Singapore, the Netherlands, and the United Kingdom. The group drafted a set of high-level principles to support the development of common digital identification systems and infrastructure and to strengthen trade agreements to facilitate the post-COVID economic recovery.

Outside of Canada, Greece, Germany, the United Kingdom, Australia and the EU are noteworthy for their digital ID initiatives.

Conclusion

Digital ID is gradually emerging in our technological societies. This is neither a breaking point nor a revolution. This emergence is an evolution and the result of advances in technology, shared learning and improved risk mitigation. As we move through the 2020s, digital ID is becoming the right tool to ensure that the identification-authentication process that's been part of our lives for decades is simple and secure.

Digital ID, by virtue of its purpose, is part of a continuum. But there is a significant change in the way it is used. People will have complete control over their personal information. It restricts the distribution of personal information in the digital space. It frees people and organizations from managing cumbersome combinations of identifiers and authenticators. And, with its decentralized structure, digital ID makes fraud much more difficult.

These concepts may seem hard to grasp in some respects. It's understandable that there may be questions and that some people are wary of new concepts that disrupt ingrained habits and behaviours in an increasingly digital world.

We need to take the time to educate the public, introduce digital ID, show how it will fit into our day-to-day lives and how it will make it easier for us to access public services or businesses. This white paper is part of the desire to foster a common understanding.

If you found the content informative, please feel free to share it.