Citizen FIRST

POWERED BY
Institute for
Citizen-Centred
Service

Digital Trust & Identity: Meeting New Expectations for Public Service Delivery

- Government Adoption of Digital ID
- Login Services as a Start Point
- Verifiable Digital Credentials for Various Data Types
- Recommendations to Advance Implementation

Image Source: utimaco.com

JOINT COUNCILS' EXECUTIVE MONTHLY REPORT

Developed by the Research Committee

October 2021

1. Introduction

This Executive Report was prepared with the guidance of Peter Watkins, the Joint Councils' Program Executive for Digital Identity at the Institute for Citizen-Centred Service (ICCS). A **digital identity ("digital ID") is a "collection of features and characteristics associated with a uniquely identifiable individual — stored and authenticated in the digital sphere — and used for transactions, interactions, and representations online**".[1]

Government organizations globally are investing in the planning and implementation of digital ID solutions. Due to the ongoing and rapid growth of digitization, new technologies and new user behaviours are transforming how government interacts with clients. This shift is dramatically changing the scope and procedures of government's identity management systems.[2]

Government organizations are beginning to re-evaluate their role in the identity supply chain, as the accurate verification and authentication of a client's identity online is becoming crucial to the functioning of society. This ability to establish and verify identities is seen as fundamental to maintaining client trust and the security of transactions.[3] The following offers a snapshot of the evolution of the internet and public sector service delivery:

Pre-Internet Era
- Paper, mail, in-person, and telephone-based service delivery
- Client information retained via paper-based documents and certificates issued by government

Digital Era
- Early stage: Informational websites, forms can be downloaded. Paper, mail, in-person, and telephone-based services delivery
- Current stage: Service delivery websites, client information retained via paper, email, and PDF format
- Digital ID means finding a way for clients to login to government websites

Digital Economy & Society Era
- Data issued to clients in a trustworthy digital form
- Clients are enabled to securely share their data across the digital economy
- Digital ID is a subset of data (in the form of verifiable digital credentials) that is issued to clients

Why is this Report Important?

- The COVID-19 pandemic ("the pandemic") has exposed the need for more contactless interactions, leading to an acceleration in the design, development, and deployment of digital identity tools and contact-free solutions.[4]
- Digital ID is a key enabler for modernizing public services (i.e. government certifications and licenses). It provides reliable authentication and enables clients to access a range of public services (online and in-person) in a faster, safer and more convenient way.[5]
- The use of reliable Digital ID verification systems reduces the risk of human error in identifying and verifying the identity of a client. It also has the potential to boost organizational efficiency, lower costs, and deliver a more favourable client experience.

What is Covered in this Executive Report?

This report includes the following:
- Introduction
- Government Adoption of Digital ID
- Login Services as a Start Point
- Verifiable Digital Credentials for Various Data Types
- Recommendations to Advance Implementation

1. The Digital Identity: What It Is + Why It's Valuable
2, 5. How governments can deliver on the promise of digital ID
3. Digital identity now: from security control to organizational enabler
4. Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations

2. Government Adoption of Digital ID

Digital IDs are the digital counterpart of physical identification (i.e. a physical ID card, passport, or driver's license).[6] It provides the credentials necessary to show that a person is who they claim to be online. A digital ID's ability to simplify interactions between clients and government can generate significant benefits. Some benefits include[7]:

1. Increasing convenience for clients by eliminating potential travel costs
2. Reducing wait-times by enabling remote online authentication
3. Enhancing administrative efficiency for government (i.e. by reducing paperwork, speeding up processing, and reducing the risk of identity fraud)

Examples of Digital ID Programs in the Public Sector

Government of Canada

The Treasury Board of Canada Secretariat (TBS) is working with other departments and jurisdictions to develop a pan-Canadian approach to digital identity and the acceptance of trusted digital identities across jurisdictions and government.[8] The goal is to allow Canadians and Canadian businesses to log in with their provincial trusted digital identity to access federal government services in a timely and secure way.

Alberta

The Government of Alberta currently has the My Alberta digital ID available to clients. MyAlberta Digital ID provides seamless access to a growing number of government sites and services, while protecting client information and privacy.[9]

British Columbia

The Provincial Identity Information Management (IDIM) program provides identity and authentication services using the BC Services Card and BCeID to support client transactions with government services.[10] These identity and authentication services are available to help clients access online services by: verifying that a person is who they say they are online and providing identity information about the person, as appropriate.

Ontario

The Government of Ontario has announced the launch of its new digital identification program that will be introduced in late 2021. The digital ID will replace physical ID cards with a digital version that can be accessed on smartphones and other devices like tablets or laptops. To do this, Ontario will be implementing a digital wallet app. Clients will be able to access their trusted government ID, which will be protected with strong encryption.[11]

6. The Benefits of Digital Identity Verification
7. Digital identity, a security imperative for governments
8. Government of Canada Digital Identity (ID)
9. MyAlberta Digital ID: A secure way to verify who you are online
10. BC Government : Identity and Authentication Services
11. Digital ID in Ontario

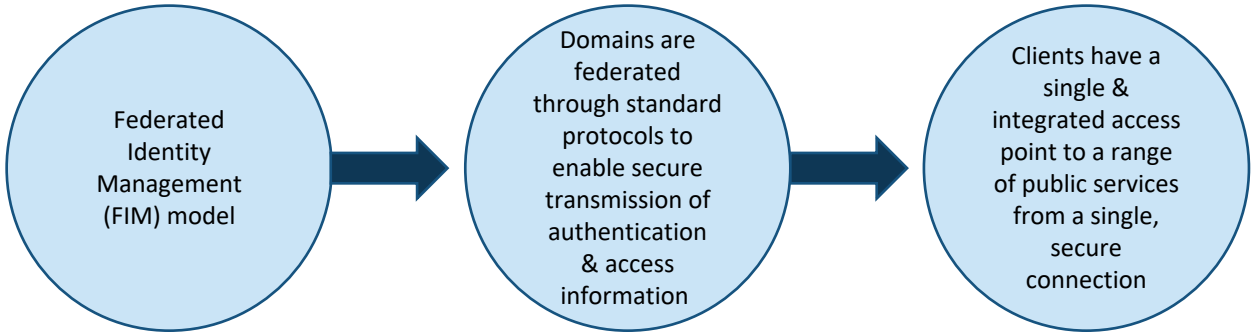
3. Log-In Services as a Starting Point

As Canadian jurisdictions continue to invest in digital ID systems, experts in the field highlight that digital ID and digital government services represent a significant aspect of the future of life in Canada.[12] Some jurisdictions are further ahead on digital ID readiness, and others are leveraging lessons learned as the demand for adoption increases.

As a starting point, many jurisdictions are focusing on establishing log-in services as a foundational component for a trusted digital ID infrastructure. Prior to the shift towards digital ID, identities were managed in silos. Clients often created several accounts on government websites and accumulated unsafe log-ins and passwords. This identity management model has been revealed to jeopardize the data privacy and security of clients and create an inconvenient user experience.[13]

To address this, governments are implementing a Federated Identity Management (FIM) model.[14] This model refers to the establishment of a trusted relationship between separate government organizations and third parties (such as application vendors or partners), which allows for the sharing of identities and authenticates users across domains. FIM enables government to provide a single sign-on (SSO) to allow clients to access multiple systems and public services online portals without the requirement to log-in to each individually.

Federated Identity Services



Privacy & Data Protection Considerations

Due to the increase of cybersecurity threats (i.e. data breaches and identity fraud) during the pandemic, there is growing public concern regarding the data privacy and security of digital ID systems. If unaddressed, these concerns present a barrier to adoption.[15]

According to privacy expert, Dr. Ann Cavoukian, governments should adopt a "Privacy-by-Design" approach to ensure fundamental protections of privacy and data security. This approach includes carefully planning data collection, creating high standards for data storage to safeguard against intrusions, and mandating user consent for all personal data use. The seven principles of the Privacy by Design methodology includes:

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**

12. Canadian privacy expert says 2021 could be the year for digital ID projects
13. Digital ID Services Platform - Enabling secure delivery of next gen digital public services
14. Single Sign-on vs. Federated Identity Management: The Complete Guide
15. How digital ID will make Canadians' data more secure: Interac + SecureKey in conversation
16. Privacy by Design: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices

4. Verifiable Digital Credentials for Various Data Types

A credential is a document that verifies that an individual has a specific attribute, qualification, or claim (i.e. passport, driver's license, or university degree). In the physical world, credentials can be verified through in-person examination of the document. However, due to the pandemic, social distancing measures has heightened the need for credentials to be verified digitally.

To address this, governments are focusing on creating user-centric Verifiable Credentials (VC) solutions to enable clients to express credentials online in a way that is cryptographically secure, privacy respecting, and machine-verifiable. There are three essential components of verifiable credentials:[17]

- Contains a proof mechanism to ensure the validity of the credential issuer and subject's claim(s)
- It is secure and tamper-proof
- Has been issued by a competent authority

Since government organizations are authoritative issuers for a broad range of important client data, they are uniquely positioned to implement VCs. To be effective, implementations must be interoperable and adhere to relevant standards, such as the W3C Verifiable Credentials Data Model. This is a set of specifications and verifiable documentation that allow credentials to be verified and shared online.[18]

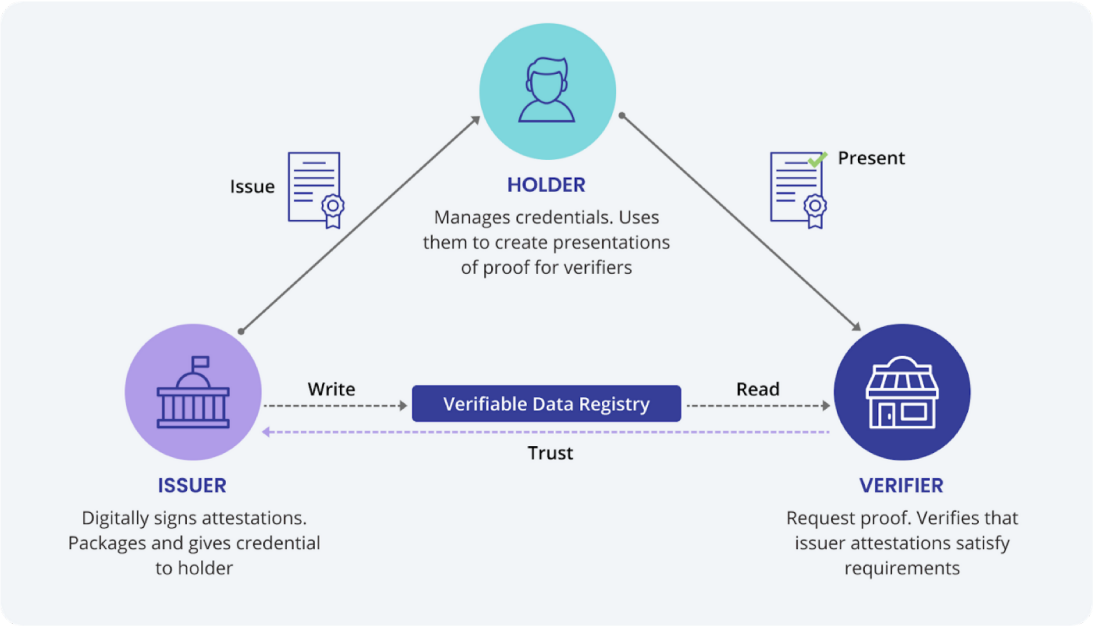
The shift towards user-centric VCs gives clients more control of their identity and data. It enables clients to hold their credentials digitally and present them to service providers as they choose. Clients are central to the triangle of trust.[19] This triangle is imperative to the functioning of VCs.

The issuer trusts the holder → **The holder trusts the verifier** → **The verifier trusts the issuer**

The Verifiable Credentials Ecosystem contains three entities[20]

Issuer	Holder	Verifier
An entity that is authorized to issue a credential (i.e. government organizations)	The individual or organization who is the owner of the credential. The holder has complete control over how the credential can be managed and with whom it can be shared, or revoked	An entity that verifies the credential and ensures it has been issued by an authorized issuer, is tamper-proof, and is still relevant (i.e. not expired or revoked). A verifier takes the verifiable presentation from the holder to determine its authenticity

Verifiable Credentials Workflow[21]



17, 21. What are Verifiable Credentials (VCs), Demystified.
18. An Introduction to Verifiable Credentials
19, 20. Verifiable Credentials Data Model 1.0

5. Recommendations to Advance Implementation

The continued growth in digital services is shifting client expectations regarding their interaction with government and private sector services throughout the economy. Clients now expect a streamlined and user-centric experience in every digital interaction.[22]

In order to meet client needs and thrive in the new digital era, governments (at all levels) need to frame digital trust and identity as a new critical infrastructure priority. Meeting the challenge requires that the necessary technical and organizational capabilities are in place to ensure the successful implementation and operation of digital trust and identity solutions.

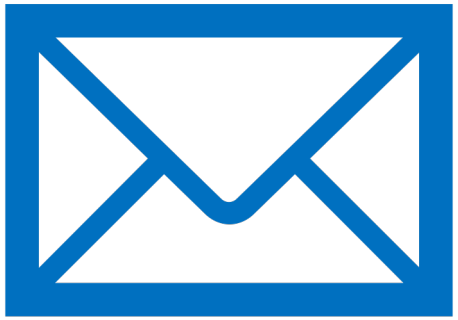
Lessons can be learned from the experience of 2021 with the design, development, and implementation of digital proof of vaccination solutions across all jurisdictions. This effort was facilitated, in part, through the Joint Councils' Priority for Digital Identity.

The experience with implementing digital proof of vaccination showed the need for five essential conditions in order to advance digital trust and identity solutions.

Conditions to Advance the Implementation of Digital Trust and Identity Solutions

1. **Mandated Priority:** Organizations should demonstrate a clear commitment and priority for providing clients with their data in a trustworthy digital form. This should be an expected feature of service delivery across all levels of government.
2. **Senior leadership:** Organizations should ensure a senior leadership role is engaged. This role should have the responsibility to engage with leaders across organizations and across jurisdictions. This is essential because implementing solutions for digital trust and identity involves aligning the priorities of multiple organizations and departments.
3. **Committed Funding:** Ensure the necessary budget is available to fund the teams and the work needed to enhance government services and the digital trust and identity infrastructure.
4. **Delivery Teams for Implementation and Operations:** Ensure there is a strong and capable in-house team of dedicated public servants to support the implementation of digital trust and identity solutions. Augment these in-house capabilities with vendor capabilities in areas such as vendor products, software development, service design etc.
5. **Open Collaboration & Alignment Across Jurisdictions:** Ensure all jurisdictions embrace the use of modern, agile/iterative, and digital methods for design, development and delivery. This will reduce risk and accelerate implementation. Openness and collaboration will improve alignment and interoperable results across jurisdictions.

22. What Government CIOs Should Know About Digital IDs



For Further Reading

- It’s time to start taking digital identity seriously
- Why A Digital ID For A Digital World Just Makes Sense
- Verifying documents & identity in the public services and beyond
- Digital identity trends – 5 forces that are shaping 2021
- The digital citizen: Improving end-to-end public service delivery via a unique digital identity

Other noteworthy articles:

UK AI strategy focused on economic growth, resilience and ethics

Concerns raised over confidentiality and transparency in government data innovation

Plugging in the User Needs For Improved Experiences

All states should become digital societies in post-pandemic era

Research Repository

Access the Citizen First Research Repository.

Recent entries on the research repository:

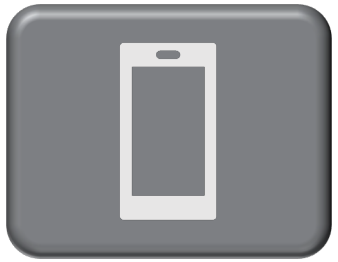
Artificial Intelligence in Government: Privacy and Human Rights Implications - Joint Councils’ Executive Report September 2021

This report explores the following: Government Applications, Privacy and Human Rights Implications, Examples of AI Challenges, Strategies for Responsible Use

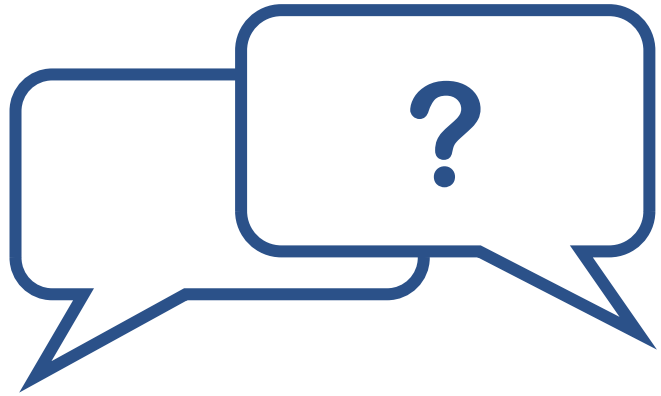
Trends in the Daily Newsletter

COVID-19 accelerated the transition to digital services, as many paper-driven processes needed to be made accessible online. Federal leaders at the GovernmentCIO Media & Research's Digital Services Series: Customer Experience virtual event noted how their agencies have harnessed the power of technology to make improvements in the overall customer experience. Human-centered design is playing a key part in various digital services

The evolution of cloud technologies and the magnitude of what they are enabling in state and local government is immeasurable—from enabling first responders in the field, vaccine distribution and tracking, to remote learning and working. As state and local governments continue their cloud modernization efforts, they face even more complex cybersecurity and compliance challenges. To manage this complexity and ensure security, state and local organizations are looking for new approaches, such as secure Multicloud-as-a-Service (MCaaS).



According to a recent announcement by Prime Minister Justin Trudeau, Canadians can now get a COVID-19 proof of vaccination form for international travel. The form is a pdf or other document. On the first page, it includes an individual's name, date of birth and COVID-19 vaccination history: which vaccines you got and when.
It also includes information on which province is issuing your proof of vaccination, a Canadian government logo, and a QR code.



We would love to hear from you!

Do you know someone who may be interested in the Joint Councils Executive Report? Please share a copy of this report. If you are not already a subscriber, you can now subscribe to receive the Executive Report by signing up. Send your questions to info@iccs-isac.org.

Follow: