



Solving the public sector identity crisis: It's time for governments to get serious about digital identities

While the tools may already exist to solve the government's identity crisis, real progress will only be made if governments significantly evolve their legacy approaches to digital identity.

Anyone who remembers having to set aside half a day to stand in line at a government office knows that we've come a long way in recent years. Today, roughly 84 percent of the world's countries provide their citizens with access to at least one online transactional service, and the global average is 14.¹

Yet, despite this progress, there is considerable work to be done before governments can deliver fully digital citizen services—a fact underscored by the scramble to remain operational during the COVID-19 crisis. It's not that the technology to shift to digital channels doesn't exist. It's that most governments lack the resources, capacity, and know-how to validate and protect their citizens' digital identities.

Although response to the pandemic arguably condensed ten years of digital innovation into six months, the move towards e-government has been haphazard at best. As countless agencies launched isolated initiatives, citizens were presented with a mishmash of access points that required them to set up unique user accounts and tolerate

multiple layers of credential checks. This is more than a cumbersome, time-consuming user experience; it's a cybersecurity nightmare.

Chief Information Security Officers (CISOs) across government sectors implicitly understand that passwords alone are insufficient protection against cybercriminals. For evidence, just consider the rising incidence of phishing, ransomware attacks, and financial fraud during the course of the pandemic.

Without sufficiently robust security postures, governments don't just struggle to protect their citizens' identities and personal information. They also stymie their own efforts to provide low-friction access to critical services. This results in substandard user experiences and stalled digital transformation efforts.

Clearly, new approaches are required.



We're still some distance from having an internationally-recognized solution that would work as easily on a government website as in a brick-and-mortar office—or a city bus. But the potential is there.

Governance, collaboration, and user control

In reconceiving the way in which digital identities are created, secured, and used, governments are coming to understand that they must go beyond the basics. Rather than simply developing solutions that give users easier access to online services—and creating ever more silos of sensitive, and often inadequately protected, private data in the process—industries are waking up to the true potential of digital identity.

As a result, the focus is now shifting from considerations about how to simplify authentication towards strategies that enable the digital exchange of verifiable identity-linked information of any kind. This requires governments to more carefully think through how they can reduce the need to store citizen data by empowering citizens to directly own and control that data.

One particular approach, Self Sovereign Identity (SSI), is fast emerging as a powerful contender for future digital identity infrastructure. With its emphasis on open-source standards, open and decentralized infrastructure, and an inverted model for data ownership, SSI allows reusable, verifiable credentials (think digitally-signed documents) to be issued directly to citizens' mobile identity wallets, rather than residing in centralized government or big-tech databases.

This empowers citizens to choose when and where to share their data, while enabling recipients to instantly verify if a digital document is signed by an authority they trust.

Turning this vision into reality, however, requires governments to create a solid governance framework. This means clarifying responsibilities for the certification, authentication, and verification of digital identity data; putting associated data protection rules and policies into place; and adopting the necessary technical standards to ensure consistency and interoperability across channels, industries, and borders.

Above all, governments will need to acknowledge that they cannot tackle this challenge by themselves. While the dangers of an exclusively private sector approach to citizen identity and data management are clear, private sector participation will still be critical to not only collectively define standards, but to build out a secure, user-friendly, and modern infrastructure that is economically sustainable.

Already, a complex ecosystem of small, high-tech innovators, large financial institutions, telecommunication providers, and technology giants is jostling to lead the way when it comes to next-generation digital identity solutions. It is these organizations that are poised to enable government initiatives, but it must fall to

government to choose wisely and develop strategy that truly serves both citizens and industry alike. As the center of gravity moves from on-premises to cloud solutions, and to edge devices like phones, the easy integration of identity solutions via Identity-as-a-Service and cloud providers is becoming widespread. Now it's incumbent on governments to organize and form collaborative private sector partnerships.

Unlocking the potential

While the tools may already exist to solve the government's identity crisis, real progress will only be made if governments significantly evolve their legacy approaches to digital identity. Notably, those that succeed will be poised to do more than simply provide their citizens with a better way to access e-government services. They can also open the door to untold levels of service innovation across all sectors of the economy. They can lay a foundation to converge services, create interoperable digital identity models, and empower citizens to control how and when to share their own data.

For the time being, we're still some distance from having an internationally-recognized solution that would work as easily on a government website as in a brick-and-mortar office—or a city bus. But the potential is there. Governments simply need to be ready to tap into it.

¹United Nations, 2020. "E-Government Survey 2020." [https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20\(Full%20Report\).pdf](https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf)

Contacts



Amir Belkhelladi | Canada Cyber Leader

abelkhelladi@deloitte.ca



Tyler Welmans | UK Blockchain Leader

twelmans@deloitte.co.uk



Alex Bolante | US Digital Identity Leader

abolante@deloitte.com



Mike Wyatt | Global Cyber Identity Leader

miwyatt@deloitte.com



Andrea Rigoni | Global Cyber GPS Leader

arigoni@deloitte.it

About Deloitte

Deloitte provides audit and assurance, consulting, financial advisory, risk advisory, tax, and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and service to address clients' most complex business challenges. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Our global Purpose is making an impact that matters. At Deloitte Canada, that translates into building a better future by accelerating and expanding access to knowledge. We believe we can achieve this Purpose by living our shared values to lead the way, serve with integrity, take care of each other, foster inclusion, and collaborate for measurable impact.

To learn more about Deloitte's approximately 330,000 professionals, over 11,000 of whom are part of the Canadian firm, please connect with us on [LinkedIn](#), [Twitter](#), [Instagram](#), or [Facebook](#).