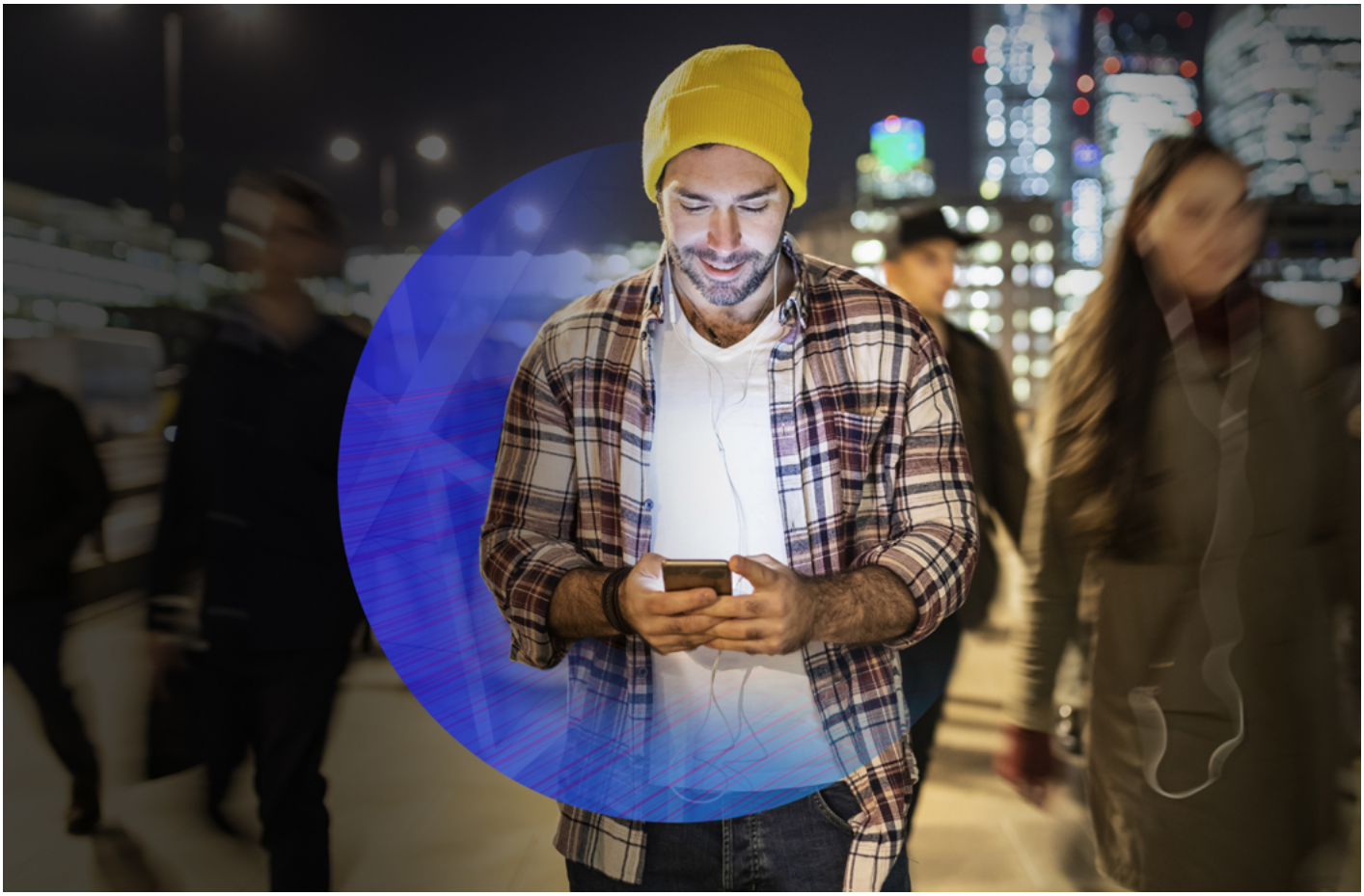
Deloitte.



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

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% of the world's countries provide their citizens with access to at least one online transactional service; the global average is 14 services.[1]

Yet, despite this progress, there's 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 the response to the pandemic has arguably condensed 10 years of digital innovation into six months, the move toward 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 over the course of the pandemic.

Without 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.

[1] United Nations, "E-Government Survey 2020", 2020.

Governance, collaboration, and user control

In reconceiving the ways 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 toward strategies that enable the digital exchange of verifiable, identity-linked information of any kind. This requires governments to 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 have them be stored in centralized government or big-tech databases.

Above all, governments will need to acknowledge they can't tackle this challenge by themselves.

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

To turn this vision into reality, however, governments need to create a solid governance framework. This entails:

- clarifying responsibilities for the certification, authentication, and verification of digital identity data;
- putting associated data protection rules and policies into place;
- adopting the necessary technical standards to ensure consistency and interoperability across channels, industries, and borders.

Above all, governments will need to acknowledge they can't 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 also to build a secure, user-friendly, and modern infrastructure that's 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's these organizations that are poised to enable government initiatives, but it must fall to governments to choose wisely and develop strategies that truly serve citizens and industry alike.

As the centre of gravity moves from on-premises to cloud solutions, and to edge devices like smartphones, the easy integration of identity solutions through identity-as-a-service (IDaaS) 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 they 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 bricks-and-mortar office—or a city bus. But the potential is there. Governments simply need to be ready to tap into it.

Visit deloitte.ca/digitalidentity to learn more about Canada's journey towards a trusted digital identity.

Contacts

Debra Sandomirsky
National Trusted Digital Identity Leader
dsandomirsky@deloitte.ca

Suzanne Robert
Trusted Digital Identity Solution Design Leader
surobert@deloitte.ca

Giselle D'Paiva
Government & Public Sector
Trusted Digital Identity Leader
gdpaiva@deloitte.ca

Deloitte.

www.deloitte.ca

About Deloitte

Designed and produced by the Deloitte Design Studio, Canada. 22-5426211.