How governments can facilitate

A new digital identity ecosystem

accenture

COVID-19 accelerated the digitization of our world—changing how we work, play and live.

Years of transformation were compressed into months. Individuals and organizations engaged in new ways. Tabled plans were greenlit overnight, and “temporary” solutions became part of our everyday lives.

Up to 55%

increase in working from home

112%

increase in digital nomads Americans since 2019

38x

growth in telehealth services

The shift exposed a gap between the digital world and the physical identity credentials we use to navigate it.

Paper-based identity no longer works in the post-pandemic world due to challenges such as:

Rise in fraud of both public and private industries

Travel bottlenecks due to manual security and ticketing

Delays in accessing government social benefits

Slow employee onboarding and more

Identity credential: an attestation to a person's identity claim, issued by an organization that has verified it. They may also detail qualifications, competencies and authority. Examples:

- Passports
- National identity cards
- Driver licenses

Source: World Economic Forum (WEF), 2021

Closing the gap with digital identity

Digital interactions will continue to rise, especially with the introduction of the metaverse and web 3.0. Behaviors and expectations are changing fast. As things evolve, governments have a dual role to play:

01

Enable and protect citizens

02

Aid the growth of the digital economy

> The imperative: to create a digital identity infrastructure that builds trust and helps to grow the digital economy.

Digital identity: a collection of verified personal attributes—name, birthdate, health status, etc.—stored digitally and trusted for use in online transactions and interactions.

Digital identity ecosystem: a network of public- and private-sector actors building ways for people to prove identity digitally across organizations.

Trust framework: a set of definitions, principles, rules and standards that all organizations in an ecosystem agree to follow. Each party's action is checked against protocols to enhance trust.

Source: World Economic Forum (WEF), 2021

Precedent for change

This isn’t the first time identity has evolved. Throughout history, we’ve adapted our methods of identification to meet the needs of an increasingly connected world.

Identity credentials have evolved significantly since their introduction.

Example: The evolution of the passport

C.450BC:
Written letters from heads of state granting leave and requesting safe passage.

15th Century:
Travel documents detailing features of individuals for travel.

20th Century:
International Civil Aviation Organization (ICAO) passport standard defined.

Today:
ePassports holding digital records of individuals, including biometric data.

Tomorrow:
Digital passports held on mobile devices as digital credentials.

With every iteration, governments have led the way, establishing trust to drive public adoption.

Trending towards transformation

Around the world, governments are funneling resources into digital identity, recognizing the need for new ecosystem-wide infrastructure. The impact of investment will be vast, clearing the path for the reinvention of processes and services.

2021

In June, the European Union updated its electronic Identification, Authentication and Trust Services (eIDAS), allowing the use of digital identity wallets on mobile devices.

2022

In January, the United Kingdom began to allow the use of certified digital identity providers in place of passports and licenses for right-to-work and right-to-rent checks.

7+

Number of governments developing or have developed trust frameworks for identity, including Africa, the EU, Australia, Canada, New Zealand, Sweden and the United Kingdom amongst others.

$80.7M

Amount France allocated to digital identity as part of NextGenerationEU.

$204M

Amount Germany have allocated to European identity ecosystem.

$600M

Amount Australia will have spent on digital identity by the end of fiscal 2024-2025.

EU: The next evolution

In June 2021, the European Union announced updates to its eIDAS framework to enable "Citizens to prove their identity from their European digital identity wallets with the click of a button on their phone". This will improve the experience for all citizens with the EU individuals and allow greater flexibility in the way they identify themselves online. However, organizations in all industries will have to rethink their processes and services to comply to the proposed changes, enabling their users greater convenience while maintaining high levels of security.

Evolving how we use identity

Originally, governments issued ID credentials for singular purposes: a passport to travel, a license to drive, etc. Now, we use them to transact and access all kinds of services.

In most countries, legislation and regulation dictate things like:

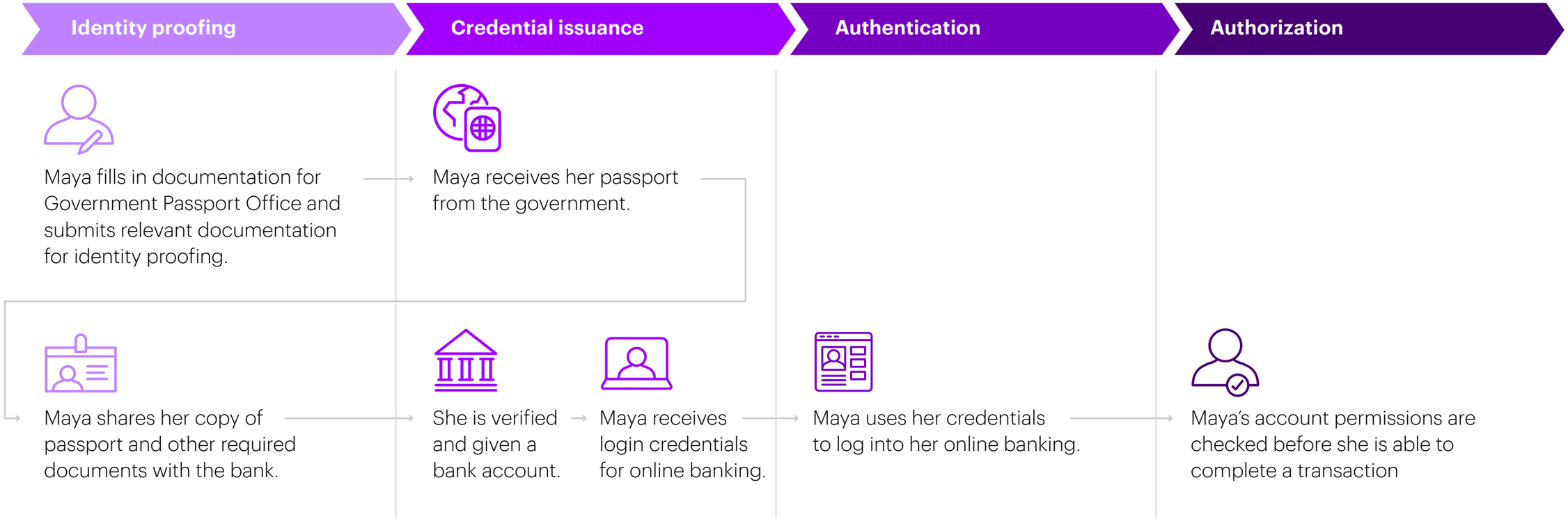
- How credentials are issued and used
- Who can issue which type of credential
- What types of transactions require them
- Who can request and verify them, i.e., regulated entities
- Which features are required within the credential

When we use our identity credentials to buy alcohol or onboard to a job, it's because the government has approved that document for that purpose. When we travel or open a bank account, we take our passports with us, assuming the airlines and banks will accept them. To us, "It just works." And governments made it happen.

Legislation instills trust. Trust leads to new behaviors and societal norms. **Our very way of life relies on government enablement of identity credentials for use outside their original purposes, across places and organizations**.

Example: using a passport in banking

Maya is looking to get a passport issued by the government to then enable her to prove her identity when opening a bank account.



Expanding digital identity for the common good

A trusted digital identity is a public good. Every sector, organization and citizen can use and benefit from it. It's now up to governments to enable and regulate the infrastructure underpinning this new evolution while protecting individual rights.

Government's are beginning to recognize this necessity. Many have already begun creating trust frameworks to enable the use of digital identity across borders, sectors and organizations. Such is the case with the European Union's revised eIDAS 2.0 regulation.

Government support and sponsorship is critical to develop, enable, safeguard and regulate these 'ecosystems and infrastructures' that are for the common good. We have identified several areas as critical actions for governments as they embark on this journey.

The key actions for governments

01 Clear policy and governance, with singular accountability

Few governments have an entity dedicated to identity. As a result, people often need different accounts to access different departments like taxation and social services. The United Kingdom has over 191 ways to set up a variety of accounts to access different services from GOV.UK, with 44 different sign-in methods.

Some use cases may justify this. Nonetheless, it's redundant, inefficient and confusing for everyone—individuals, private companies and the departments themselves.

A single body, accountable for identity across agencies through well-defined governance, would drastically streamline things. Working across the public and private sectors, this group would take the lead on things like:

- Unifying and owning the agenda
- Determining policy
- Clarifying the strategy
- Creating a framework
- Engaging with the private sector

02 Legislation and regulation for trust and acceptance

A successful identity ecosystem infrastructure requires both physical and digital forms of ID to be legally valid. Why?

01 Legislative validation creates trust, enabling us to freely accept digital credentials as we do traditional ones.

02 This universal acceptance drives adoption and leads to the reinvention of processes, services and experiences.

To that end, legislation and frameworks must include a standard definition of digital identity and a common set of clear rules.

> Additionally, governments must work domestically and abroad to enable acceptance in digital environments that span physical boundaries.

03 Public-private collaboration around use cases

When it comes to defining use cases and driving adoption to unlock value, governments are mission critical.

Some use cases exist entirely due to regulation, like proving identity to open a bank account (e.g., know your customer regulation). Naturally, governments must be involved in any case where digital credentials are used like physical ones for compliance.

Most use cases will cut across sectors, requiring coordinated solutions. Examples:

- Traveling across borders
- Buying retail goods
- Sharing credentials and qualifications with organizations
- Confirming age to access goods and services

In these cases, the government's ability to bring parties together in service of the common good is key.

It's equally important that sectors refrain from creating their own identity systems that won't work elsewhere. Doing so would create identity silos and friction between them. As fragmentation is the enemy of adoption, collaboration must happen sooner rather than later.

> Digital identity ecosystems: unlocking new value
> Our executive guide outlines how to prioritize use cases, build ecosystems and deliver value. Published in partnership with WEF.

Anatomy of an MVP use case

Use cases that are key to drive adoption share two common factors:

High friction in the user experience means greater potential for individual adoption, as well as efficiency savings for organizations.

High frequency of use makes the opportunity ripe for reuse and adoption.

04 Cooperation across borders and sectors

The value of digital identity can't come to fruition without international partnership. After governments agree on standards and definitions among frameworks, they should experiment in lock-step.

Take cross-border travel, a key use case. What good is a passport that's valid in one country but not another?

The passport is one of the most interoperable credentials in the world. Governments made it viable by working together through the ICAO. The digital equivalent requires a similar effort, using existing international infrastructure as a springboard for progress.

The good news? Cooperation is already underway with initiatives like the ICAO's Digital Travel Credentials (DTC) project. Several nations are also testing cross-border digital identity:

Canada and the European Union

Australia and Singapore

Germany and Spain

05

Flexibility and responsible innovation

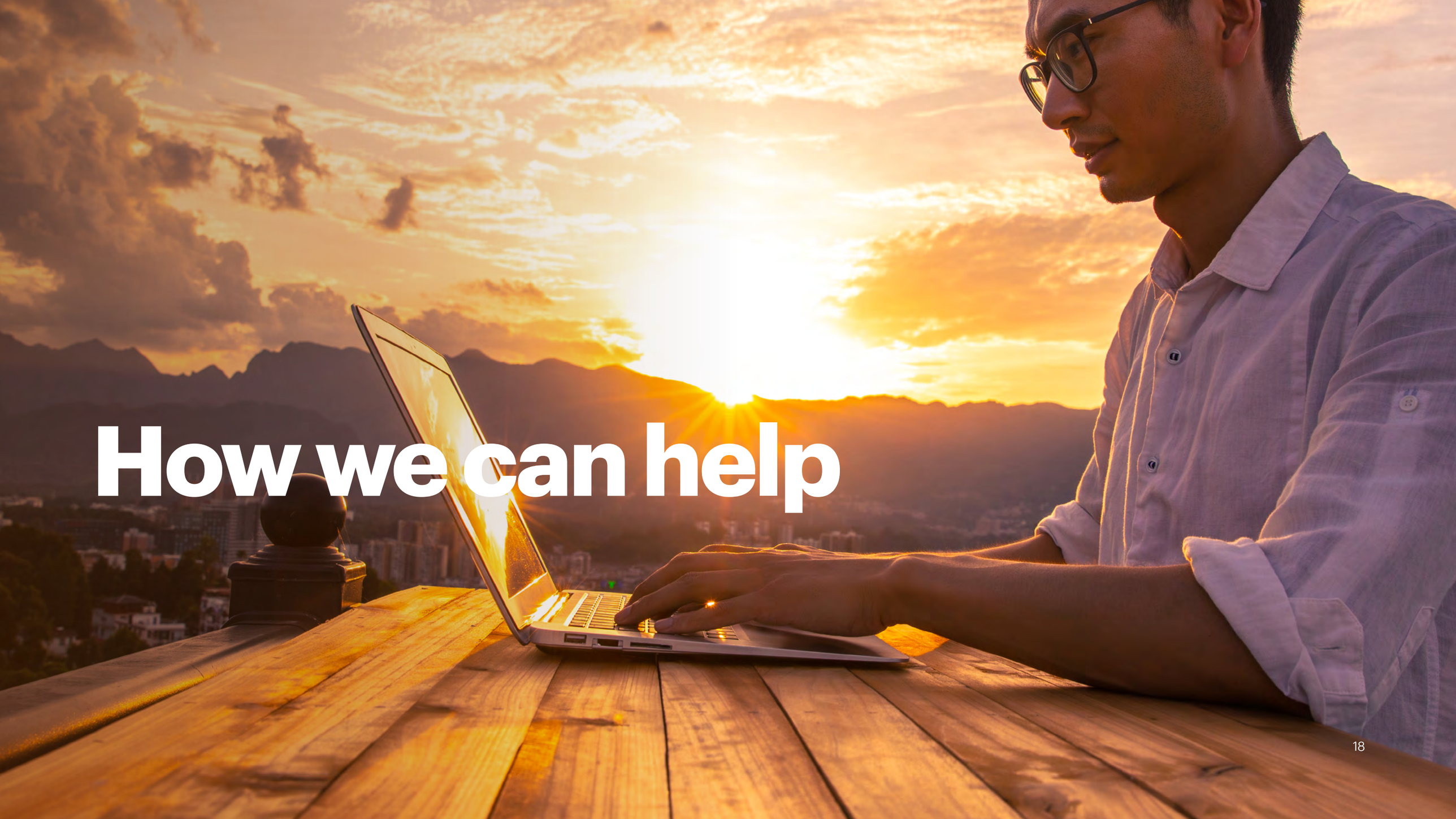
Digitization is blazing ahead, and digital identity is riding the tide. Governments must keep up—but they must do so responsibly and with a new level of agility.

Responsibility

Protecting citizens is the government's duty. As digital identity is a public good, they must push for ethical private-sector innovation. Advocacy begins with a guiding set of principles that support privacy, safety and security along with individual rights and freedoms.

Agility

As the metaverse and Web3 expand, so will the volume of digital interactions that span geographic boundaries. Regulation will be anything but easy. Governments must be ready to anticipate the next wave of innovation, instilling the right guide rails for the benefit of organizations and citizens alike.



How we can help

For more than 50 years, Accenture has helped governments embrace innovation, including across the citizen identity landscape.

We have partnered with leading organizations to advance the field, including:

- World Economic Forum, launching programs like Known Traveler Digital Identity for seamless air travel
- Standards bodies and global organizations like the World Wide Web Consortium and Trust Over IP
- Public and private organizations spanning travel, health, supply chain, finance and more

Accenture have unparalleled experience from setting the agenda, to defining the standards, to implementing solutions for Digital Identity. We bring our deep expertise and experience to help advise Governments on the current landscape, plan, support and implement deployments in an array of projects and lay out the next steps for future technological advances, such as digital identity ecosystems. Together, we help governments and partners co-create solutions that can launch them to the forefront of the digital horizon.

Authors

Christine Leong
Managing Director, Global Decentralized Identity and Biometrics Lead

Jack Keeling
Tech Innovation Strategy Manager, .NEXT Identity, Tech Innovation Group

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Technology and Operations services and Accenture Song—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 710,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

About Technology Incubation Group

The Technology Incubation Group—currently focused on blockchain and multiparty systems, quantum computing and extended reality (XR)—is made up of a team of highly specialized strategists, consultants, architects, developers and entrepreneurs. The group works with key business leaders to fundamentally shift their strategies and models using collaboration, innovation and vision to drive real business results. The incubation process spans both technology and business to create Accenture's next offerings for the future and developing new markets, working with other groups within Accenture, including Technology, Strategy & Consulting, Interactive and Operations.