Digital identity trends – 5 forces that are shaping 2020

thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/trends

Last updated: 23 September 2020 - Estimated reading time: 11 minutes

Digital identity is well and truly established as one of the most significant technology trends on the planet.

Indeed, for a growing number of public stakeholders and citizens, it's already a day-to-day reality. As a result, a revolution in the way that individuals interact with public institutions is underway.

And the private sector is fast getting in on the act too.

In this dossier, we'll highlight the five key digital identity trends that are set to shape the landscape in 2020 and beyond.

We'll see in a video from Davos 2019 the foundational role of digital identity in the digital economy.

But first, let's look back at some of the landmarks of 2016-2018.

Digital ID milestones for 2016-2018

Before we look to the future, let's review the big ideas that gained traction in the past two years. This overview will provide some reliable indicators as to where we are heading.

National ID schemes increased in number, visibility, and reach

- The UN and World Bank ID4D initiatives set a goal of providing everyone on the planet with a **legal identity** by 2030.
- Numerous new National **eID programs** (including card and mobile-based schemes) were launched or initiated. Examples include new projects in Algeria, Belgium (mobile ID), Cameroon, Ecuador, Jordan, Kyrgyzstan, Italy, Iran, Japan, Senegal, Thailand, Turkey, major announcements in Afghanistan, Denmark, the Netherlands, Bulgaria, the Maldives, Norway, Liberia, Poland, Jamaica, Sri Lanka, Zambia and a pilot scheme in Myanmar. Some of these programs now include **biometrics**, the majority in the form of fingerprints.
- Schemes such as the Gov.UK Verify initiative started in 2016, and Australia announced that the first phase of its digital identity program was launched in August 2017.
- **France** also announced early 2018 its national eID scheme for fall 2019.
- **Canada** is also progressing with its federal digital identity scheme named Pan-Canadian Trust Framework, piloted by the Digital ID Authentication Council of Canada, a non-profit organization (DIACC). A federal proof of concept project for a unified login authentication service called **Sign In Canada** started in the fall of 2018.
- **Aadhaar (India's national eID scheme)crossed the 1 billion users mark in 2016.** At the end of 2018,1,2B Indian residents got their Aadhaar ID (99% of adults), a digital identity that can be obtained based on their biometric and demographic data.

New technologies and regulations supporting the transformation ahead

- Digital driver's license projects (also known as mobile driver's licenses) gathered momentum in countries including the USA, UK, Australia, and the Netherlands.
- Early tests of blockchain technologies took place: in Estonia, to aid the development of a ground-breaking transnational e-residency program; in the UK, to see how it can be used to help make efficient welfare payments to citizens. Blockchain-based **self-sovereign identity** has been explored for decentralized digital ID architecture since 2018.
- **Smart borders/smart airports** emerged at a faster pace. Combined with the 1 billion ePassports now in circulation, and a strong push behind biometrics (particularly face recognition), they offered travelers a taste of cross-border movement that is as secure as it is swift and seamless.
- The European Union's Electronic Identification and Signature (eIDAS) regulation came into force in July 2016, requiring mandatory cross border recognition of electronic ID by September 2018.

New standards emerged, fostering compatibility and interoperability.

- A new ICAO working group on digital travel credentials was created, led by Australia.
- The LDS2 conception phase – 'the future of the ePassport' - was undertaken by the ICAO NTWG Logical Data Structure 2 Sub-Group.
- The ISO SC17 WG10 - Task Force 14 "Mobile Driving Licence" started to work on verification standards for Mobile DL and defined the scope of off-line verification. 2018 will see draft specs of both off-line and on-line verification appear for a new work item.
- The IATA mobile ID working group was constituted in 2016 and started in 2017.
- The US Commerce Department's National Institute of Standards and Technology (NIST) awarded a federal grant to support further the development of trusted identities based on the Digital driver's license.

Digital identity - 5 forces that shape 2019-2020

To start with, don't expect any slow down in the momentum we've experienced over the past two years.

The next two years will see some of the most accelerated evolutionary changes experienced so far by public stakeholders and their partners in the field of secure digital identity.

In particular, we think that these changes represent essential considerations for authorities that want to make digital identity and on-line services (particularly mobile services) defining features of their modernization processes in the years to come.

We expect to see:

1. More **mobility** and **access to the Internet**
2. Greater demand for **security** and trust

3. An accelerating shift towards smart **cities**
4. More calls for **public** supervision of **digital identification systems**
5. Even more National ID card and eID programs , national ID initiatives, and implementations

Let's dig in.

#1 Mobile communication dominates

ID **will become ever more mobile**. Of course, it doesn't take an expert to recognize we've entered an era in which mobile connectivity dominates. But it's worth emphasizing that the trend shows no sign of abating. And the implications for digital ID are profound.

Look at some of the facts:

- Over **4 billion people** already have access to the Internet in early 2020. The global online Internet penetration will reach 60% by the end of this year.
- **50% of global internet traffic is mobile in 2020,** according to Statista. Mobile devices (also including tablets) are now the primary means of accessing the internet for users.
- Google – a company that knows a thing or two about the future of technology - is steadily moving towards a **mobile-only world.**

The lesson for all digital ID stakeholders is clear: prepare for **mobile-first** solutions.

#2 Guaranteed security: Private data, public framework

We'll **expect nothing less**. Identity is the link that connects an individual to his or her community.

For public authorities, the key challenge in the next two years will be to create harmonious digital bonds that secure the relationship between new mobile identities and broader society.

This bond is only possible through a general **framework of trust**, built on guarantees of personal data protection and security.

In 2018-2020, we've seen and will continue to see that measures taken to bolster security and combat fraud are generally well accepted by citizens. These are, of course, sovereign matters par excellence.

The Cambridge Analytica revelation mid-2018 was (once more) a good illustration for the need for a robust digital identity framework, privacy by design and regulation.

Facebook offered none of the seven principles of Privacy by Design.

These predictions are confirmed by what we discovered about expectations for mobile security, in interviews conducted with 1300 citizens in November 2016.

Robust security measures will be the response to new demands for trust in all exchanges between citizens and public authorities.

In terms of privacy protection, the General Data Protection Regulation of May 2018 (GDPR) for the European Member States represents a significant step forward for data protection and privacy. Twenty-eight countries are impacted, **including the UK**.

Yes, you read that right. 500m persons have the same law.

In August 2017, India's supreme court ruled privacy a "*fundamental right*" in a landmark case, illustrating that biometric data protection is now on top of regulators' list in the largest democracy of the world.

Modi's new government enhanced privacy protection laws in 2019.

The California Consumer Privacy Act(CCPA) voted at the end of May 2018 is now effective as of 1 January 2020. It's is a significant step forward for privacy rights as the state is often seen as a trendsetter in this domain.

The law is potentially a model for **a US (i.e., federal)data privacy law**. In that sense, the CCPA has the potential to become as important as the GDPR.

And New York State now stands beside California with its Stop Hacks and Improve Electronic Data Security (in short SHIELD) act, effective on 21 March 2020.

Privacy demands rigorous accountability. **We saw** in 2018-2020 **the emergence of a global consensus,** its fundamental principle being that mismanagement of personal information will not be tolerated and that companies that do not protect data adequately could be hit with massive fines.

Read more on GDPD, CCPA, and SHIELD in our dossiers on data protection regulations.

Take a look at these key takeaways:

- Citizens are willing and waiting for greater security.
- 2020 represents a **perfect opportunity for public authorities** to revitalize the 'sovereign bond' with citizens. In doing so, they can prove it is not some obscure relic of the past, but a symbolic, identity-rich vehicle for collective trust.

#3 The smart city will become our playground

Around the world, the shift of populations to urban environments is already one of the defining trends of the 21st century. Inevitably, technological developments are becoming inextricably linked with this mass migration.

The digital or the smart city is becoming the model that ensures consistency in all the links between urbanites, their broader communities, and public authorities.

This model includes, of course, eGovernment or mGovernment, within which digital identity is the key that unlocks the individual's access to a rich array of services and support.

Or, to put it another way, the smart city is set to become our new playground.

By their very nature, smart cities are mobile environments. The digital ID will, therefore, represent the 'virtual umbilical cord' that continuously links each individual to their public and social life.

The message for public authorities is clear: **national digital ID creates an unrivaled opportunity for local creativity.**

So here's another key takeaway.

> Think national, act locally. In a mobile-only world, local services become even more relevant.

#4 Public supervision will be critical to sustaining growth in the digital economy

Faced with an increasingly challenging economic landscape, governments are inevitably searching for new opportunities for sustainable, harmonious growth.

As regulatory environments take shape, **close collaboration between the financial world, central and local public authorities, and digital communications operators** will support effective solutions and implementation of best practices.

Of course, the real source of new business opportunities is not digital identity itself, but **the myriad of applications** it enables. This domain is where banks and other operators will see a bottom-line return on their investment.

As already outlined, the march of the digital ID is well underway. The focus will, therefore, be on the adoption of the new structures and regulations that are needed to govern the associated services and transactions.

So what does this mean in practice?

The role of public authorities in 2018-2020 will be to:

- Build and nurture national momentum.
- Support and coordinate local government investments through which local transformations, close to the community, can operate effectively and efficiently.
- Make sure that these multiple local initiatives create a coherent and interoperable spectrum of solutions: wherever they may be, mobile citizens will need to find similar modes of service.

In the years ahead, the market will follow these initiatives.

How can we be so sure?

Because evidence of uptake of digital ID and associated services are multiplying, giving us the most explicit signals since the concept was first introduced some fifteen years ago that a tipping point has been reached.

#5 Three-stage dynamics will drive digital ID pilots and roll-outs

The digital ID evolution – as broad as it is dynamic - will continue to move forward. The citizen is the fundamental driver of these changes.

Millennials now make up a majority of employees and a growing proportion of total citizen populations. They are **reshaping the culture of our institutions**. Ultimately, this tech-savvy generation is being proved right.

The older generations, by finally joining in and adopting these forms of technology, can break out of their isolation, stay in contact, and preserve social and especially family bonds.

For 2018-2020, we see equally strong dynamics across the following three stages:

- From theory to proof-of-concept: 2018 and 2019 will be the year of proof-of-concept for the **blockchain in public services** - specifically in areas such as **e-government** and **health care**. Questions on the real interest of self-sovereign identity for digital identity will be answered.
- From proof-of-concept to pilot: As it moves from a proof-of-concept technology into secure and interoperable solutions with new standards, 2019 and 2020 will be the "years of the pilot" for **digital driver's licenses,** digital credentials **on mobile, and virtual/digital cloud passports.**
- From pilot to implementation: Countries will move more quickly than expected, and we could reach a tipping point over the next 24 months. Many national ID schemes are approaching critical mass.

The benefits of digital identity

Digital identity is playing a foundational role in our digital economy. Discover more with the video below from the World Economic Forum (Davos 2019).

Watch Video At: https://youtu.be/1-V7lyxrOmw

Now it's your turn

2020 holds many changes in store.

Indeed, we can't claim to predict all the essential issues and topics that will emerge in the year to come.

Can you fill in some of the gaps?

If you've something to say on national digital ID trends, a question to ask, or have found this article useful; please leave a comment in the box below. We'd also welcome any suggestions on how it could be improved or proposals for future papers.

We look forward to hearing from you.