Research Paper

Digital Identity:

Concepts, State of Play, and Its Role in the Data-Sharing Economy

Research Paper by Wirecard
in collaboration with Innopay

Contents

01.0 / Introduction

The digital identity concept is no longer new. It has been widely discussed due to its significance in the digitalization of economies and in the development of emerging economies. All over the world, public and private digital identity initiatives have sprung up, competing for identity owners and the parties that rely on identities. Nevertheless, there is still a lack of understanding of the principal workings of digital identity. Similarly, there is little awareness about the role digital identities must play as data transactions between industry players increase exponentially and secure and scalable ways of sharing data will be required to cater to this development.

With this research paper, Wirecard, in collaboration with Innopay, aims to create a better understanding of what digital identity is and how it currently plays out in the market. Furthermore, we want to put forward our vision of the role of digital identity going forward.

First, the basic concepts of digital identity are explained (section 2). Next, we present a framework of digital identity models and the principal characteristics that help to characterize and qualify existing initiatives (section 3). In sections 4 and 5, the global landscape of identity initiatives is described, followed by a deep-dive into the European landscape. The final section explains the link between digital identity and data sharing: It provides an outlook on the role that digital identity will need to assume as we move toward an economy in which data transactions, more than ever before, are omnipresent drivers of economic growth.

02.0 / Basic concepts of digital identity

An identity is a collection of characteristics, or attributes, that make a given individual, entity, or object unique and recognizable over time ("uniqueness" and "sameness"). Similarly, a digital identity is a representation of an individual, entity, or object through a standardized set of attributes in the digital world.[1]

Attributes that make up a digital identity can belong to different categories:

Attributes	Examples
Inherent permanent	Biometrics
Assigned permanent	Name and national ID numbers
Assigned non-permanent attributes	Address or phone number
Historical data	Medical or credit histories, purchasing behavior
Inferred data	Creditworthiness based on personal profile / history

Table 1: Categories of attributes
Source: Innopay analysis

Inherent and assigned permanent attributes are usually considered core elements of a digital identity. In addition, authenticators such as passwords or fingerprints are used to determine whether the claim to a certain identity is valid.

The attributes making up the digital identity, together with a given degree of confidence that these are true, provide the trust required to conduct a digital transaction. We can therefore define digital identity as follows:

"Digital identity is a standardized set of attributes representing an individual or legal entity, used to facilitate digital transactions by providing trust."

A digital identity possesses three basic functions that enable the use of the identity in any type of digital transaction: identification, authentication, and authorization.

Identification ("I claim to be X")

Identification is either the claim of who someone is by stating it (self-declaration), by what others state about someone (assertion), or the confirmation of an identity officially assigned by a trusted third party (i.e. passport, driver's license, bank, notary).

During the identification process, certain attributes representing an entity are assigned to a specific identity.

Authentication ("I am the one who claimed to be X")

[1] For the purpose of this paper, we will not consider identities of objects (as opposed to individuals or legal entities).

Authentication is the action of proving that someone is who they claim to be. The most common form of verifying an identity in the digital world is the entry of a password, i.e. the proof of secret knowledge.

This can be both cumbersome and insecure, since many people use the same password with a low level of difficulty for many accounts. The emergence of new technologies such as biometrics, an increased importance of data privacy, and regulatory developments such as PSD2 (in particular the requirements for strong customer authentication, SCA) have made a case for multifactor authentication procedures.

A multifactor authentication uses two or more independent factors combined to give a higher level of assurance, which can also be dynamically requested based on the risk profile of inquired transactions.

Frequently used factors

Knowledge	Something you know (password, PIN, secret question)
Possession	Something you have (chip card, token, computer, phone)
Inherence	Something you are (biometric: fingerprint, face recognition, typing pattern, voice)

Additional factors

Location	Where you are (GPS, IP-address, mailing address, phone line)
Behavior	Actions, gestures etc. that are unique to you
Relationship	Who vouches for you (reputation system, social identity, ID networks)

Table 2: Authentication factors (non-exhaustive)
Source: Innopay analysis

With successful authentication, someone has verified to a certain level of assurance to be the claimed identity.

Level of assurance (LoA) describes the level of certainty with which a relying party can assure that the digital identity belongs to the natural or legal person claiming to be the owner of that identity. This, in turn, depends primarily on the quality of the authentication, as well as on the quality of the initial identification during registration. Different levels of assurance are required depending on the context and purpose of an authentication, for example, logging onto a social media platform will require a lower LoA than opening a bank account, which is subject to regulatory requirements such as AML. Various frameworks exist that classify levels of assurance in different ways. One framework, for instance, is provided by the eIDAS regulation, which classifies LoA levels as low, substantial, and high.

Authorization (“As X, I am allowed to do / I authorize Y”)

Authorization is the process of granting access to certain resources or permission to carry out certain actions based on a given identity. During the process, it is determined what someone is allowed to access or to do.

In combination, the processes of identification, authentication, and authorization establish the trust necessary for digital transactions and enable a multitude of secondary functions of digital identity, including registering for a service, logging on, sharing attributes, electronic signing, performing age verification, and many more. Thus, digital identity sets the cornerstone for very many interactions in a digital economy.

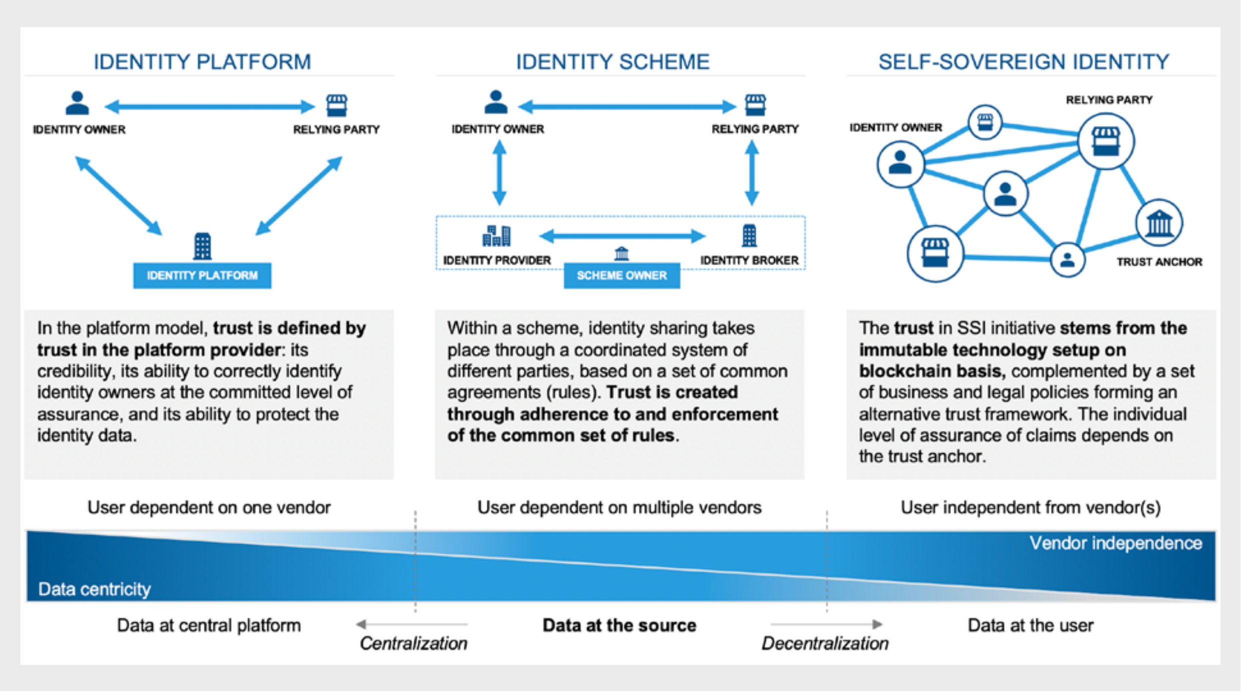
03.0/ Digital identity models

Digital identity—and trust as a central component of digital identity—can be organized in various ways, starting with basic bilateral relationships between identity owners and relying parties, to models allowing the sharing of identities across a broad range of parties and services.

Today's world of creating digital trust is mainly characterized by direct or bilateral relations between the identity owner and the relying party (the entity that relies on the identity, for example, to provide a certain service). Examples are any online services (online shops, social networks, etc.) where the identity owner has directly registered for an account. In the direct model, trust is dependent on the relying party's proprietary processes for identification, authentication, and authorization, as well as on the identity owner's perceived trust in the relying party. In this model, relying parties are in full control of their onboarding and identity maintenance processes, but this also comes with the burdens of cost, effort, and risk.

Without a digital identity framework spanning multiple players, identity owners are confronted with multiple time-consuming registration processes and the need to remember many different login credentials.

If there is an arrangement between multiple parties that enables the sharing of trustworthy attributes, identity owners can profit from single sign-on (SSO) systems that enable a single authentication process across multiple IT systems and organizations. Furthermore, relying parties can profit from efficiency gains and reduced costs and risks. Such systems are called federated digital identity systems. In a federated digital identity system, there are various models to determine trust, and they differ in their degree of centralization of data and their independence from a specific vendor (see figure 1).



In the platform model, **trust is defined by trust in the platform provider**: its credibility, its ability to correctly identify identity owners at the committed level of assurance, and its ability to protect the identity data.

Within a scheme, identity sharing takes place through a coordinated system of different parties, based on a set of common agreements (rules). **Trust is created through adherence to and enforcement of the common set of rules.**

The **trust** in SSI initiative **stems from the immutable technology setup on blockchain basis,** complemented by a set of business and legal policies forming an alternative trust framework. The individual level of assurance of claims depends on the trust anchor.

Figure 1: Archetypical models of federated identity
Source: Innopay analysis

Identity platform

In the platform model, an identity platform facilitates the exchange between identity owner and relying party. It allows the identity owner to register and create an identity with the platform provider, which shares the identity with connected relying parties upon the identity owner's request.

Because platforms rely on networks, they must aim at onboarding a critical share of both sides of the market—identity owners and relying parties—to their platform. If a critical mass is not reached, a platform will fail. By nature, users of an identity platform are highly dependent on one vendor, i.e. the platform provider (low level of vendor independence), while the platform provider also centralizes the identity data that flows across the platform (high level of data centricity).

Trust arrangement:
In the platform model, trust is defined by trust in the platform provider: its credibility, its ability to correctly identify identity owners at the committed level of assurance, and its ability to protect the identity data.

Examples:
Examples of identity platforms include relying parties that provide an identity service for third parties (e.g. Facebook login), newly created platforms dedicated to identity services (e.g. Verimi), and governments that provide extensive identity services based on official government IDs (e.g. mobile ID in Estonia).

Identity scheme

Within a scheme, identity sharing takes place through a coordinated system of different parties and roles, based on a set of common agreements. Identity owners store their identity at an identity provider, which, at the request of the identity owner, shares it with a designated relying party. Sharing is done through the role of a broker, which connects the identity provider and the relying party. As opposed to a platform, the identity owner and the relying party do not have to contract with the same party, and there can be multiple players fulfilling the roles in the framework, instead of one. Typically, a scheme owner ensures compliance with the scheme rules and admits participants to the scheme. As such, it resembles payment schemes such as Visa, Mastercard, or iDEAL (in the Netherlands).

Multiple actors are involved in a scheme, so that users are less dependent on one actor than is the case with a platform. Additionally, data is stored at its source, i.e. at various different actors involved in the scheme and therefore avoids the centralization of data. As with a platform, the success of a scheme relies on networks. The involvement of multiple actors can be a positive factor in scaling a scheme to a viable size, but a sound governance of the multiple actors involved is a critical factor.

Trust arrangement:
In an identity scheme, trust is created through adherence to and enforcement of the common set of rules.

Examples:
Examples of identity schemes include the Dutch bank-driven identity scheme iDIN, Sweden's BankID and the United Kingdom's government-led initiative GOV.UK Verify.

Self-sovereign identity

The notion of self-sovereign identity (SSI) is a relatively new digital identity concept driven by increasing privacy concerns and the emergence of enabling technology, that is, blockchain (see box: "The case of blockchain for digital identity"). Self-sovereign identity aims to return full control over the digital identity to the identity owner by storing it at the individual user level. This usually happens in a secure device memory or in a cloud where only the specific user has access.

It is important, however, not to confuse self-sovereign with self-sufficient. In order to provide a verified identity, external bodies such as banks or the government (known as "trust anchors") are still needed to testify that a given identity is valid. Each verification attestation, known as a verified claim, is stored separately. Zero-knowledge proofs, testified on a blockchain, make it possible to store private data locally while proving its authenticity when it is shared.

As with the other models of federated identity, any SSI initiative also requires a critical mass of identity owners and relying parties to gain any relevance in the market—the classic "chicken and egg" problem. Interoperability with other initiatives through standardized claims can be one way of achieving network effects. At the same time, sound business models are required to create sustainable SSI systems.

Trust arrangement:
The trust in an SSI initiative stems from the immutability of blockchain technology, complemented by a set of business and legal policies that form an alternative trust framework. The individual level of assurance of claims depends on the trust anchor.

Examples:
Many initiatives relating to the concept of SSI are currently not beyond a proof-of-concept phase. However, some prominent examples, such as Sovrin and uPort, are driving the development of SSI. Very recently, big techs, too, have entered the space of SSI: Microsoft is incubating ideas around self-sovereign identity together with standardization bodies such as W3C, while Samsung has teamed up with several financial services firms and mobile carriers to develop a blockchain-based mobile identification system.

While there are barely any SSI-related initiatives beyond proof-of-concept stage today, various identity platforms and schemes have entered the scene in recent years and are already operational. While platforms are a viable strategy choice particularly for individual players that already have a strong presence on the relevant market, a scheme setup facilitates the involvement of a broad spectrum of players in an economy. This, as we argue in the final section of this paper, is an important characteristic as the digital economy evolves toward a data-sharing economy—and suitable digital identity systems are bound to become all the more important.

The case of blockchain for digital identity—a way toward decentralized identity

Generally, blockchain or DLT is a technology protocol that allows data to be shared directly between entities in a decentralized peer-to-peer network. By nature of its decentral, immutable, and transparent infrastructure, it creates trust among relying parties through the technology itself and eliminates the need for a centralized broker, which is required, for instance, in a platform model.

In identity, blockchain has potential applications as a decentralized, secure information storage and a traceable, immutable routing and transfer mechanism. It functions as a distributed protocol, giving users the ability to safely create and store their identity attestations on a shared ledger and expose them to different RPs in a peer-to-peer manner.

These capabilities make the application of blockchain a perfect fit for the implementation of the concept of self-sovereign identity. Based on blockchain infrastructure, SSI allows users to maintain control over their identity data. With the possibility of generating blockchain addresses, it offers the possibility for users to create their own, unique digital identifiers (DIDs). DIDs can then be complemented with attestations from various stakeholders (these might be various entities ranging from an individual related person to banks or governments) to increase the level of assurance for the respective identity. In the SSI world, anyone with a decentralized identity can issue a credential or an attestation for anyone else (though these will naturally carry different levels of assurance depending on the nature of the source).

Blockchain offers the possibility to safely store identity data, related credentials, and attestations on a distributed ledger and share them with relying parties. By putting hashes on the blockchain, credentials can also be notarized, that is, equipped with a time stamp and an electronic seal. Furthermore, blockchain offers the potential to link credentials to smart contracts to, for example, trigger automatic payments and other value-added services.

Example:
One of the most prominent examples in the application of blockchain in digital identity is uPort. uPort is building a blockchain-based open identity system to realize the concept of self-sovereign identity. It builds on the Ethereum blockchain and allows users to register their own identity, send and request credentials, sign transactions, and manage their keys and data via a mobile wallet. uPort has partnered with the city of Zug to create the first blockchain-based government identity system that allows users to register their digital identities on a distributed ledger and access government services with their uPort app.

04.0/ Digital identity around the world

Around the world, we can find various forms of the digital identity archetypes discussed in the previous section. Most governments are moving toward the digitization of national identities and an increasing number thereof are thinking about comprehensive digital identity systems to facilitate the digital transformation of society. The market landscape of commercial digital identity services is shaped by a variety of players from different industries. They include banks, non-bank players such as telcos, and specialized digital infrastructure providers, ranging from start-ups to large corporations and consortia. Public-private partnerships are also emerging, where many private initiatives are based on digital national identity systems or government institutions are accepting private digital identity services as a means of authentication for their citizens.

This section aims to provide an overview of relevant initiatives around the world, followed by a closer look at Europe.

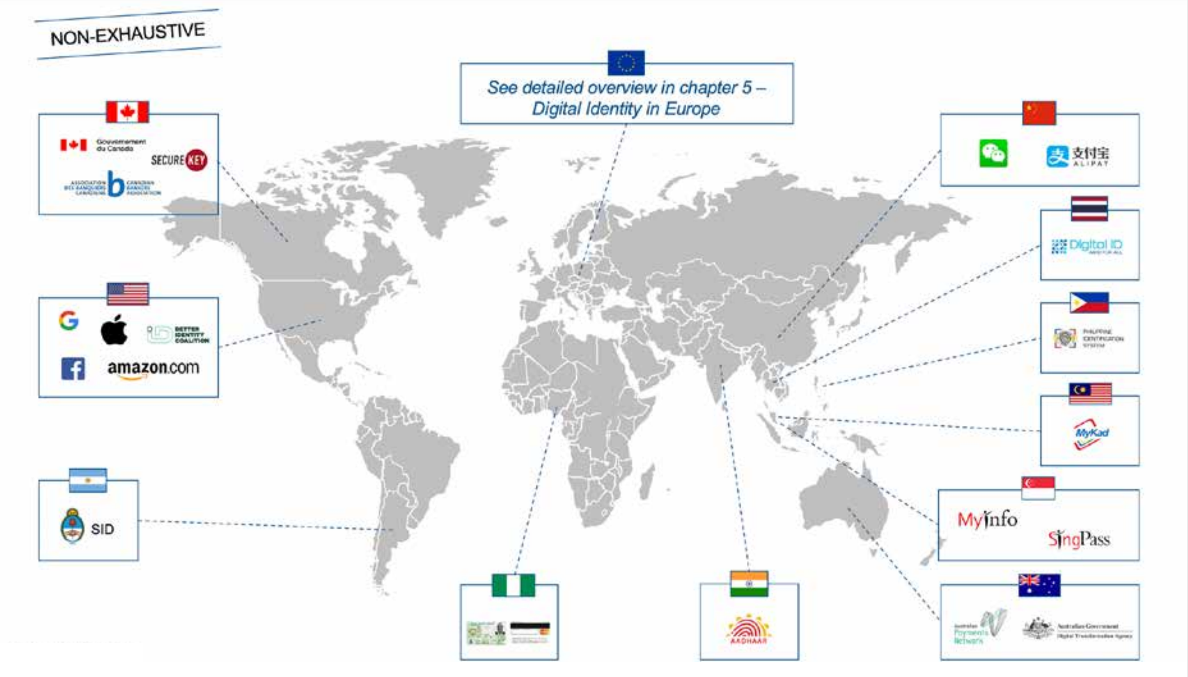

NON-EXHAUSTIVE
See detailed overview in chapter 5 – Digital Identity in Europe
Gouvernement du Canada
SECURE KEY
Association des Banquiers Canadiens
b
Canadian Bankers Association
Better Identity Coalition
amazon.com
SID
AADHAAR
支付宝 ALIPAY
Digital ID
Philippine Identification System
MyKad
MyInfo
SingPass
Australian Payments Network
Australian Government Digital Transformation Agency

Figure 2: Overview of digital identity initiatives worldwide
Source: Innopay analysis

Americas

The US digital identity space is dominated by private sector initiatives from big techs. All GAFA[2] companies are leveraging their platform capabilities to provide digital identity services, not only in the United States, but also globally. In particular, Google and Facebook have created prominent identity services with Facebook Login and Google Login. With these services, users can log into a website with their existing Facebook/Google credentials and thus skip cumbersome registration procedures. However, since the data is not generally verified (in other words, it is self-declared data from virtual accounts at Facebook or Google) and only provides low level-of-assurance, these login services only apply for third-party services and products that do not require legally compliant user identification. A digital identity system for higher LoA use cases is not yet widely available. However, an initiative from a cross-sectoral consortium of companies (including Bank of America, JP Morgan, IDEMIA, Mastercard, and Onfido) called "Better Identity Coalition" recently released a research paper calling for a policy change that reduces barriers to creating a "better" digital identity system in the United States[3].

In Canada, too, calls for a federal digital identity system are increasing. The Canadian Bankers Association has released a research paper on Canada's digital identity future[4], the Digital Identification and Authentication Counsel of Canada has outlined key principles for a digital identity ecosystem in Canada, and the government has signed a memorandum of understanding (MOU) with Estonia—a role model for a government-initiated digital identity system. Additionally, there is a prominent private-sector initiative from the major banks called Verified.Me by Secure Key, which uses blockchain technology for a decentralized digital identity approach[5].

In South America, Argentina stands out. The country has launched the Digital Identification System (Sistema de Identidad Digital, SID), a government initiative, in close cooperation with the banking sector. The system aims to provide access to government services through remote biometric authentication with facial recognition. There are also plans to extend the service into the health sector[6].

[2] *GAFA is an acronym that stands for Google, Apple, Facebook and Amazon.*
[3] *See The Better Identity Coalition (2018)*
[4] *See Canadian Bankers Association (2018)*
[5] *See BNN Bloomberg (2019)*
[6] *See OECD (2019)*

Asia

From the implementation of a single identity card to blockchain-based eID systems, South-East Asia provides quite a diverse picture of digital identity systems. In general, government initiatives, often initiated as part of broader digital transformation programs of nation states, set the tone for digital identity.

For instance, Malaysia became the first country in the world to use an electronic ID card (MyKad) in 2001 that, besides a photo identification, also includes biometric fingerprints on a computer chip. The card can be used to access government agency services as well as for public transport. Malaysia also announced the launch of a new digital ID platform to complement its current system and enable easy and secure access to e-commerce and financial services[7].

The Philippines are currently running a PoC for their new Philippine Identification System (PhilSys), which aims for a central identification platform and a single identity card that includes biometric information such as fingerprints and iris scan (currently the Philippines have about 33 different ID cards in use)[8]. The system includes use cases such as tax transactions, voting, and opening a bank account[9].

Thailand has adopted a bill to create a new digital ID system (National Digital ID, NDIDI) that enables the electronic identification and authentication of the end-users of their services by relying on derived identification from another member of the system[10]. The new scheme, developed in cooperation with 10 commercial banks, aims to provide a route of communication between members (that is, relying parties and identity providers) in a way that can eliminate the need to undertake repeated KYC processes[11]. For that purpose, the system relies on blockchain technology with decentralized nodes connecting each member. In the first phase, the service will mainly focus on payment and banking services and healthcare[12].

In Singapore, the National Digital Identity system (NDI) is set to launch in 2020 and aims to enable Singapore residents and businesses to transact digitally with the government and private sector in a convenient and secure manner. The system includes a digital authentication service to access government services (including 2FA), a mobile app SingPass enabling fingerprint and facial recognition for login, and the service MyInfo enabling auto-fill for online forms. The NDI program aims to establish a platform infrastructure, including a developer portal (NDI api), with which the private sector can build value-added services on top. These services currently include cross-border mobile remittances, credit card applications, and the purchase of life insurance.

In China, digital identity is pushed mainly through big platform players from the private sector—similar to the United States—although there is closer cooperation with the public sector. Most digital transactions occur within the ecosystems of Tencent and Alibaba. Tencent owns the mobile messaging service platform WeChat, while Alibaba owns the mobile payment app Alipay. Both platforms have built ecosystems that allow users to transact online and offline with merchants that accept payments via WeChat or Alipay. WeChat and Alipay together have a 93.3% penetration of the entire mobile payment population in Mainland China[13]. This has made the case for both providers to enter the digital identity space. Following a trial with the city of Guangzhou, citizens will soon be able to use WeChat digital ID cards for accessing government and other services across the country. Alipay is following a similar approach by launching pilots of its new WebID service in the cities of Quzhou, Fuzhou, and Hangzhou[14].

[7] *See CIO (2019)*
[8] *See Gulf News (2018)*
[9] *See Philstar Global (2018)*
[10] *See The Nation Thailand (2019)*
[11] *See CIO (2019)*
[12] *See Bangkok Post (2019)*
[13] *See WALKTHECHAT (2019)*
[14] *See SecureIDNews (2018)*

Asia

Turning to India, the country provides one of the most notable examples of government-initiated eID programs. The Aadhaar Act is the world's largest human identification number scheme, linking a uniquely generated identification number (unique identification number, UID) to personal data and biometric details of over a billion people stored in a central database[15]. With this digital identity, Indian citizens not only have access to government services but also to mobile and financial services (for example, opening a bank account). The introduction of UPI (Unified Payments Infrastructure) in 2016 in combination with Aadhaar has proven to be a sound foundation for FinTech innovation in India.

Australia

Australia is making the case for close cooperation between the private and public sector and is moving toward a model of public-private partnership (PPP).

The Digital Transformation Agency is building a scheme-like model—the Trusted Digital Identity Framework—which is a set of rules and standards all providers within Australia's digital identity ecosystem must adhere to[16]. The ecosystem comprises a set of identity providers such as myGovID, where the government acts as the identity provider, and intends to also integrate identity providers from the private sector, such as banks and Australia Post. In the first phase, the scheme-like framework allows access to government services, but the program aims to expand into further relying services, such as banking, in the near future.

In 2019, the banking industry came together to develop a separate yet interoperable digital identity trust framework, which is expected to engage private identity providers to a greater extent.

In parallel, Australia is pioneering the empowerment of citizens to re-use their personal data stored at companies across various economic sectors (including banking, energy, telecoms, insurance, retail, and others) under the framework of its Consumer Data Right Act[17]. This approach is similar to Europe's PSD2, but extends the scope of controlled and open data access to other sectors. The act is expected to further accelerate the adoption of digital identity.

Africa

The African Union (AU) has recently recognized digital identification systems as an essential infrastructure to unlock access to profound new social and economic opportunity, such as education, employment, financial services, mobile communication, travel, and voting . The Union aims to promote the development of digital interoperable national identity systems across the continent.

With its national ID card launched in 2014 in cooperation with Mastercard, Nigeria has chosen to implement a digital identity solution in a PPP format. The national card includes functionalities such as strong electronic authentication and digital signature, biometric identification, and payment functionality. However, the current identity system is very fragmented, and adoption of the identity card is less than 1%. This is why the government, in close cooperation with the World Bank, has set up a strategic roadmap for a digital identity ecosystem in Nigeria.

[15] *See CNBC Africa (2019)*
[16] *See Digital Transformation Agency (n.d.)*
[17] *See The Treasury (n.d.)*
[18] *See CNBC Africa (2019)*
[19] *See Premium Times (2014)*
[20] *See NIMC (2017), p. 8*

05.0 / Digital identity in Europe

Drivers of digital identity in Europe

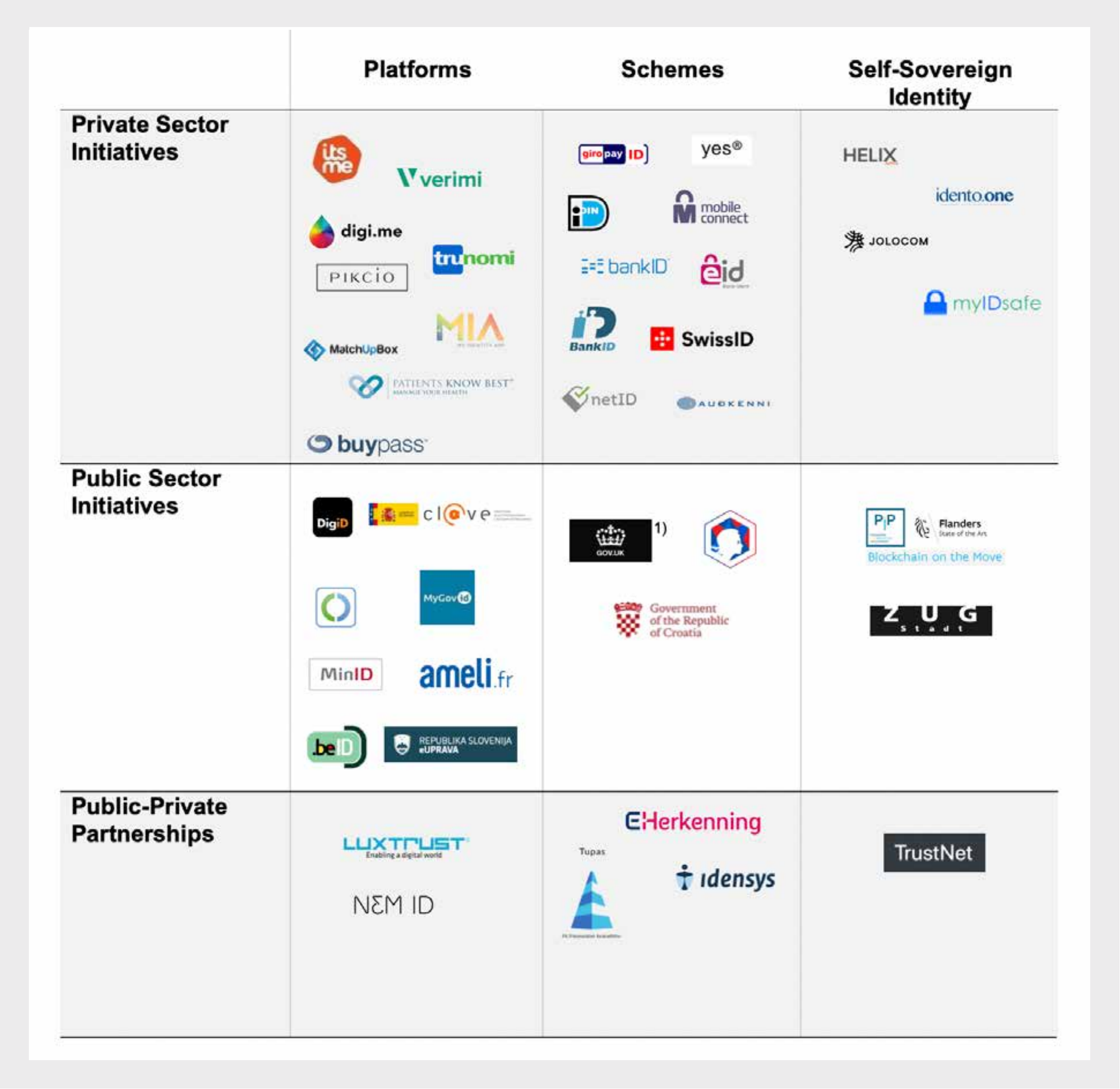
Europe is probably the most mature and diverse region for digital identity systems and solutions in the world. One reason for this high maturity is that almost all countries have managed to digitize their official identity services. This basically sets the cornerstone for the successful implementation of digital identity systems that include access to e-government services.

Another driver of digital identity in Europe is the effort being made to harmonize legal digital identity frameworks through the eIDAS regulation. eIDAS enables secure and seamless electronic (cross-border) interactions between businesses, citizens, and public authorities. This is supported by further regulation such as the General Data Protection Regulation (GDPR) and the second amendment to the Payment Service Directive (PSD2). GDPR harmonizes data protection laws across European Union member states, protects and empowers citizens with regard to data privacy, and reshapes how organizations deal with data privacy. Thus, it contributes to creating a framework for digital identity systems in the EU. PSD2, in turn, opens up new possibilities through standardized access to bank account information. PSD2 obliges banks to grant regulated third-party service providers access to the payment accounts they manage in online banking, including the retrieval of data about the account holder. With the use of qualified website certificates and qualified seals for the identification of third-party service providers (TPPs), PSD2 also applies to the structures created by eIDAS.

The European digital identity landscape

These developments have spurred the emergence of various digital identity systems that apply different archetypes of identity models across Europe. However, when we look at Europe as a whole, the result is a rather fragmented identity landscape.

The following table gives a categorized overview of the fragmented digital identity landscape in Europe.



	Platforms	Schemes	Self-Sovereign Identity
Private Sector Initiatives	itsme verimi digi.me trunomi PIKCIO MIA MatchUpBox PATIENTS KNOW BEST buypass	giropay ID yes® iDIN mobile connect bankID eid BankID SwissID netID AUÐKENNI	HELIX idento.one JOLOCOM myIDsafe
Public Sector Initiatives	DigiD cl@ve MyGovID MinID ameli.fr beID REPUBLIKA SLOVENIJA eUPRAVA	GOV.UK 1) Government of the Republic of Croatia	P|P Flanders State of the Art Blockchain on the Move ZUG Stadt
Public-Private Partnerships	LUXTRUST Enabling a digital world NƐM ID	EHerkenning Tupas idensys	TrustNet

Notes: This is a non-exhaustive overview of initiatives based on public information available in English. Not all listed initiatives fully resemble the archetypical models explained in section 2.

[1)] In October 2018, GOV.UK Verify announced a handover to the private sector after a transition period of 18 months.

Source: Innopay analysis

The table above shows a diverse picture of private sector initiatives, with various companies exploring different models for digital identity systems. Public sector initiatives are currently more focused on a platform model, with scheme-like models gaining ground when private sector players are integrated into national e-identity systems (in moves toward a PPP model, see, for example, UK.GOV Verify). For SSI, it will be particularly interesting to see how SSI-related public sector initiatives play out in the future. Here, the city of Zug, Switzerland, boasts one of the most mature setups to date[22].

[21] *See Public Technology (2018)*
[22] *See Consensys (n.d.)*

Estonia

In Europe, some public sector-driven initiatives clearly stand out. For instance, Estonia is one of the leading countries that launched e-ID—almost two decades ago. Today, 98% of Estonians have an e-ID card and the system facilitates authentication, data storage and sharing, and digital signatures through its chip-based cards or digital keys[23]. The e-ID card offers a wide array of services and is embedded in Estonians' everyday lives. The e-ID card has increased efficiency for Estonians in many areas, ranging from using it as a national health insurance card, logging into bank accounts online, online voting, checking medical records, and filing taxes.

The Nordics

The Nordics, too, have rather mature digital identity systems in place. In Denmark NEM ID, in Finland FINeID, and in Norway MinID: The public sector issued digital identity methods many years ago. In addition, successful private sector solutions, mainly driven by financial services institutions, have been created in Scandinavia (Sweden—BankID, Norway—bankID, Finland—Tupas). Sweden, for example, has successfully implemented a federated digital identity scheme owned by a coalition of banks. Eight million people use BankID on a regular basis for a wide variety of private and public services. In Sweden, 80% of the adult population has a digital identity and, through the use of BankID, an individual can open a bank account, declare their taxes, and sign contracts[24].

The Netherlands and Belgium

The scheme model proved successful in the Netherlands, too, where the major banks have joined forces to build iDIN, a digital identity system that was built on the infrastructure of the existing, highly successful payment scheme iDEAL. iDIN supports a login service, identification (merchants can retrieve specific user attributes), and age verification (to check if a user is over 18)[25]. In line with the value proposition of BankID, iDIN also started to provide digital signing services in 2019. Additionally, Dutch citizens also use the government-initiated DigiD solution to access public services. DigiD is well accepted, but currently provides only a limited level of assurance, which is expected be upgraded in the future.

One of the Netherlands' immediate neighbors has implemented another successful private sector scheme. In Belgium, the itsme app allows users to confirm their identity and approve transactions online. itsme is operated by the four leading banks and major telco operators in Belgium. The system can therefore combine the possession of a mobile phone (and SIM card) with the banks' know-your-customer (KYC) data[26]. Furthermore, itsme has worked in close cooperation with the government right from the start. Today, itsme is integrated into many public services, such as social security or tax administration.

[23] *See E-Estonia (2019)*
[24] *See BBVA Research (2018)*
[25] *See iDIN (n.d.)*
[26] *See De Meersman (2019)*

The benefits of close cooperation between the private and public sector are also illustrated through another Dutch initiative—eHerkenning. The eHerkenning scheme focuses mainly on B2G and B2B relationships by facilitating identification, authentication, and transactions between companies and government services[27]. A crucial feature is the role-based functionality of people vis-a-vis a legal entity.

At the heart of eHerkenning lies the public-private partnership between the Ministry of Interior Affairs and the business community. The login system is not a single technical tool but is provided by several accredited suppliers that form part of a network. These work according to mutual agreements around technical-, legal- and business-related aspects.

Germany

Besides the public sector initiative around the German e-ID card, where citizens can utilize an electronic ID card to access government services online via a card reader or smartphone application, three private sector initiatives mainly stand out. Verimi—a cross-sector joint venture of German blue-chip companies including Deutsche Bank, Telekom, Daimler, and Lufthansa—provides a digital identity platform, where users can register once and reuse their identity data at various partners across industries to log in, register, and sign documents[28]. Additionally, a set of German media players has joined forces to create the login scheme called netID. Because, for now, the service focuses only on login functionality, it can be compared to the services of Facebook and Google[29]. Another private sector initiative uses a scheme model to leverage banks' data and capabilities around KYC to offer digital identity services. Under the name of YES, public banks in Germany (Sparkassen and Genossenschaftsbanken) have formed a coalition to create a digital identify scheme comparable to BankID or iDIN.

[27] *See eHerkenning (n.d.)*
[28] *See ASQUARED (2018)*
[29] *See Identity Economy (2019)*

Self-sovereign identity in Europe

So far, only a few pilot projects and proofs of concept for SSI are in development in Europe. The following examples give a non-exhaustive overview of the SSI landscape in Europe:

- In Austria, a consortium of financial service providers, a telco provider, a media company, Austrian Post, and the Austrian Retail Association are developing a PoC for an SSI solution under the name of myIDsafe. The concept is based on Sovrin's digital identity and common open source standards.
- In Germany, the Berlin-based start-up Jolocom has developed an open-source protocol for the decentralized sharing of digital identity data. Additionally, Jolocom has built an app that allows users to securely manage their identity data in a mobile wallet.
- In Finland, a research project called "TrustNet" is exploring the use of SSI in a network of research institutions and industry partners. TrustNet is a pilot project for decentralized personal data management, where the sandbox environment is also provided by the Sovrin Foundation.
- In Switzerland, the city of Zug, which is also known as the "crypto valley," has partnered with uPort to build an SSI solution for its citizens that works on the Ethereum blockchain. With the SSI implemented in Zug, users can pay their parking fees, register for elections, or sign into e-government services online.
- In Belgium, a project called "Blockchain on the Move" is piloting SSI and its application at municipal level. It explores the potential of SSI for e-government use cases and state-issued credentials for private sector B2B and B2C use cases. Initiated by the government, it also aims to examine the opportunities for public-private partnerships at a later stage of development.

A call for harmonization and interoperability

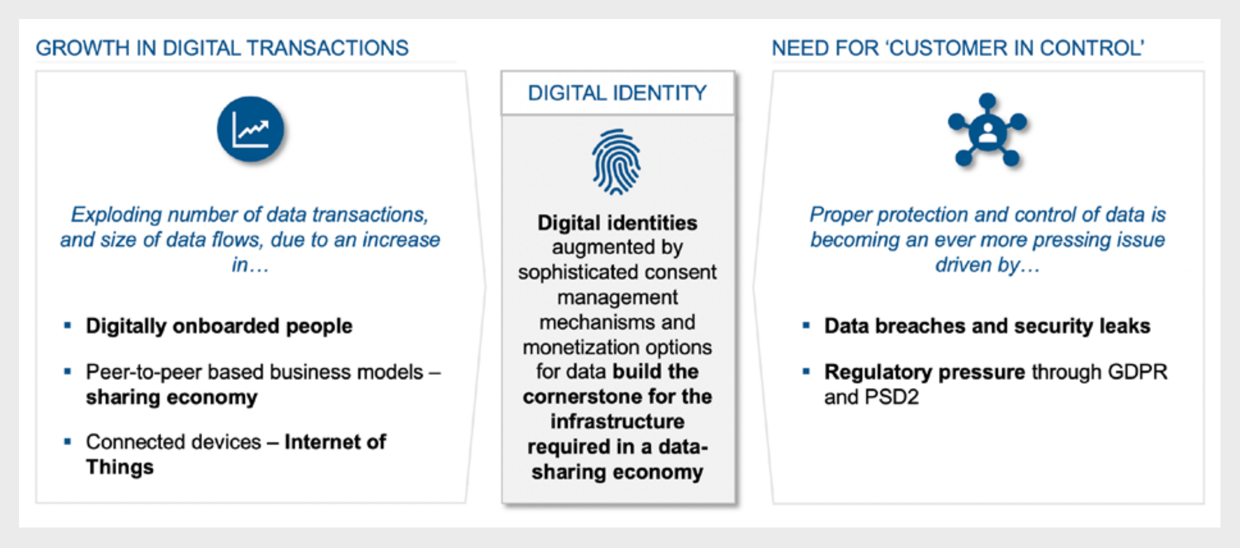
The digital identity landscape in Europe is evolving dynamically and innovation is occurring at a strong pace. At the same time, fragmentation is high, and consolidation is both likely to occur and necessary for digital identity to deliver on its value proposition. In the meantime, dedicated service providers that aggregate identity methods for relying parties can help improve the reach of individual methods on the side of the relying party. The role of governments varies and ranges from full-fledged identity provider (for example, Estonia) through creating a concrete legal framework (for example, Switzerland, Sweden, Norway, and the Netherlands) to a more passive stance (for example, Germany).

Either way, broad and interoperable digital identity is necessary as data transactions between economic actors increase exponentially, all of which need to be enabled and secured by trusted digital identities. Building on regulatory efforts formed under eIDAS, private and public sector need to strengthen collaboration toward a more harmonized and interoperable landscape of digital identity in Europe.

06.0 / Digital identity’s role in the data-sharing economy

The most fundamental function of digital identity, in its various manifestations, is to provide the trust required to conduct digital transactions, including payments, log-in and signing. In varying degrees, depending on context and setup, digital identity solutions can increase convenience, promote security, and ensure regulatory compliance. Initiatives based on trust frameworks (schemes) rather than single platforms have the potential to get a wider range of players within the economy involved, fulfilling different roles in a broad identity infrastructure that serves as enabler of today’s—and tomorrow’s—digital economy.

While this type of infrastructure is an advantage today—though, in many countries, as shown above, it is not yet fully a reality—it will become essential in the years ahead. This need is driven by two fundamental developments: the explosion of digital data transactions throughout the world and the increasing need to put data under the control of its owners.



GROWTH IN DIGITAL TRANSACTIONS

Exploding number of data transactions, and size of data flows, due to an increase in…

- **Digitally onboarded people**
- Peer-to-peer based business models – **sharing economy**
- Connected devices – **Internet of Things**

DIGITAL IDENTITY

Digital identities augmented by sophisticated consent management mechanisms and monetization options for data **build the cornerstone for the infrastructure required in a data-sharing economy**

NEED FOR ‘CUSTOMER IN CONTROL’

Proper protection and control of data is becoming an ever more pressing issue driven by…

- **Data breaches and security leaks**
- **Regulatory pressure** through GDPR and PSD2

Figure 3: Digital identity’s role in the data-sharing-economy
Source: Innopay analysis

The number of data transactions, and correspondingly the size of data flows, will increase exponentially in the coming years. The major driving forces behind this include the growing number of people worldwide who adopt digital services, the rise of the sharing economy, and the Internet of Things.[30]

At the same time, enabling proper protection and control of data is becoming an ever more pressing issue. The introduction of the EU General Data Protection Regulation (GDPR) in 2018 was a result of increasing privacy concerns. It, too, has made it evident that personal data, as well as being an asset, is also a liability for the businesses controlling it. Those who fail to comply with the standards set forth by the GDPR run the risk of being severely penalized by regulators, in addition to the reputational damage caused when discovered. For data shared between businesses, the need for proper data protection is self-evident in the light of competitive and commercial considerations.

[30] *See the forthcoming book “Everything Transaction”: Liezenberg, Lycklama, Nijland (2019))*

Further regulation concerns access to data: While PSD2 is forcing the European banking sector to open up account data, laws to open up other sectors are likely to be passed in the future. In Australia, the Consumer Data Rights Act already does so today, and other governments have substantially developed their thinking in this direction.

Companies can respond to the dilemma between the increasing availability of data and the need to secure it by using data sovereignty as their guiding principle. Data sovereignty is about putting customers' data under the customers' control. Proper customer control, however, requires the ability to obtain verifiable consent. And, in turn, the key ingredient for providing "verified control" of data by customers is digital identity.

As data is increasingly shared between businesses and individuals, as well as among businesses, a proper identity and consent infrastructure based on data sovereignty is fundamental for a move from today's digital economy toward a safe and prospering "data-sharing economy." This infrastructure should feature trusted digital identities augmented by sophisticated consent management mechanisms, as well as monetization options for data. Also, it should be characterized by a clear separation of data from actual applications. Much like a payment works irrespective of the goods purchased, the identity-based sharing of data should be independent of the actual data and its specific use.

Several projects exist, such as the Solid initiative by Tim Berners Lee, inventor of the World Wide Web, that are currently working in this direction. Furthermore, sector initiatives such as iSHARE, a B2B data-sharing scheme designed for logistics, already provide data and use-case agnostic mechanisms for sharing data between multiple parties in a standardized and legally sound way, based on identification, authentication, and authorization.

The path ahead will require increased collaboration within and between economic sectors, as well as across borders, ensuring alignment on an identity and consent infrastructure that is convenient, secure, and widely adoptable. Financial institutions, and the financial sector as a whole, can play a key role in these efforts. Secure infrastructure, highly verified customer identities, their expertise of transactions, and above all their experience with providing trust put them in the pole position to facilitate the structural shift ahead.

[27] *See eHerkenning (n.d.)*
[28] *See ASQUARED (2018)*
[29] *See Identity Economy (2019)*

07.0/ List of references

- ASQUARED. 2018. E-Identity Solutions in Europe—A European Overview. https://asquared.company/en/blog/e-identity-solutions-in-europe-an-european-overview-769/.
- Bangkok Post. 2019. Digital ID scheduled for year-end. https://www.bangkokpost.com/business/1703996/digital-id-scheduled-for-year-end.
- BBVA Research. 2018. Digital Identity: the current state of affairs. https://www.bbvaresearch.com/en/publicaciones/digital-identity-the-current-state-of-affairs/.
- BNN Bloomberg. 2019. Canada's banks launch SecureKey's Verified.Me digital identity network. https://www.bnnbloomberg.ca/canada-s-banks-launch-securekey-s-digital-identity-network-1.1251979.
- Canadian Bankers Association. 2018. White Paper: Canada's Digital ID Future—A Federated Approach. https://cba.ca/embracing-digital-id-in-canada.
- CIO. 2019. Which countries are implementing digital IDs in SE Asia? https://www.cio.com/article/3331296/which-countries-are-implementing-digital-ids-in-se-asia.html.
- CNBC Africa. 2019. As more Africans go online this is what needs to be done to protect their identities. https://www.cnbcafrica.com/zdnl-mc/2019/06/18/protecting-the-identity-of-africans-in-a-common-digital-market/.
- Consensys (n.d.): Zug Digital ID Case Study: Government Issued Blockchain Identity. https://consensys.net/enterprise-ethereum/use-cases/government-and-the-public-sector/zug/.
- Digital Transformation Agency (n.d.): Trusted Digital Identity Framework. https://www.dta.gov.au/our-projects/digital-identity/join-identity-federation/accreditation-and-onboarding/trusted-digital-identity-framework.
- De Meersman, Ivo. 2019. "Discover itsme®: Belgian digital ID". https://www.europeanpaymentscouncil.eu/news-insights/insight/discover-itsmer-belgian-digital-id.
- E-Estonia. 2019. https://e-estonia.com/solutions/e-identity/id-card/.
- eHerkenning (n.d.). https://www.eherkenning.nl/english.
- Gulf News. 2018. National ID to substantially save cost for Philippines. https://gulfnews.com/world/asia/philippines/national-id-to-substantially-save-cost-for-philippines-1.2217535.
- Identity Economy. 2019. "Spezialisierte Identity-Dienstleister werden an Bedeutung gewinnen—Interview mit Karl Illing (Innopay)". http://identity-economy.de/spezialisierte-identity-dienstleister-werden-an-bedeutung-gewinnen-interview-mit-karl-illing-innopay (German content).
- iDIN (n.d.). https://www.idin.nl/en/.
- Liezenberg, Chiel; Lycklama, Douwe; Nijland, Shikko. 2019. Everything Transaction. Innopay management book forthcoming in an English version in September 2019.
- NIMC. 2017. A Strategic Roadmap for Developing Digital Identification in Nigeria. https://www.nimc.gov.ng/docs/reports/strategicRoadmapDigitalID_Nigeria_May2018.pdf.
- OECD. 2019. Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector. https://www.oecd.org/gov/digital-government/digital-government-review-argentina-key-findings-2018.pdf.
- Philstar Global. 2018. What you need to know about the proposed national ID. https://www.philstar.com/headlines/2018/05/29/1819744/what-you-need-know-about-proposed-national-id#PbHAUxbck9ToShlT.99.
- Public Technology. 2018. Government to hand GOV.UK Verify over to private sector and cease funding. https://www.publictechnology.net/articles/news/government-hand-govuk-verify-over-private-sector-and-cease-funding.

- Premium Times. 2014. SCANDALOUS: Outrage in Nigeria as government brands National ID Card with Mastercard's logo. https://www.premiumtimesng.com/news/headlines/167479-scandalous-outrage-in-nigeria-as-government-brands-national-id-card-with-mastercards-logo.html.
- SecureIDNews. 2018. Chinese digital ID comes to Alibaba's payment app. https://www.secureidnews.com/news-item/chinese-digital-id-comes-to-alibabas-payment-app/.
- The Better Identity Coalition. 2018. Better Identity in America: A blueprint for Policy makers. https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/5b4fe83b1ae6cfa99e58a05d/1531963453495/Better_Identity_Coalition+Blueprint+-+July+2018.pdf.
- The Nation Thailand. 2019. Banks to ride on digital ID scheme with new services. https://www.nationthailand.com/business/30373220.
- The Treasury (n.d.): Consumer Data Right. https://treasury.gov.au/consumer-data-right.
- TIME. 2018. India Has Been Collecting Eye Scans and Fingerprint Records From Every Citizen. Here's What to Know. https://time.com/5409604/india-aadhaar-supreme-court/.
- WALKTHECHAT. 2019. The cross-border payment war of WeChat Pay and Alipay. https://walkthechat.com/the-cross-border-payment-war-of-wechat-pay-and-alipay/.