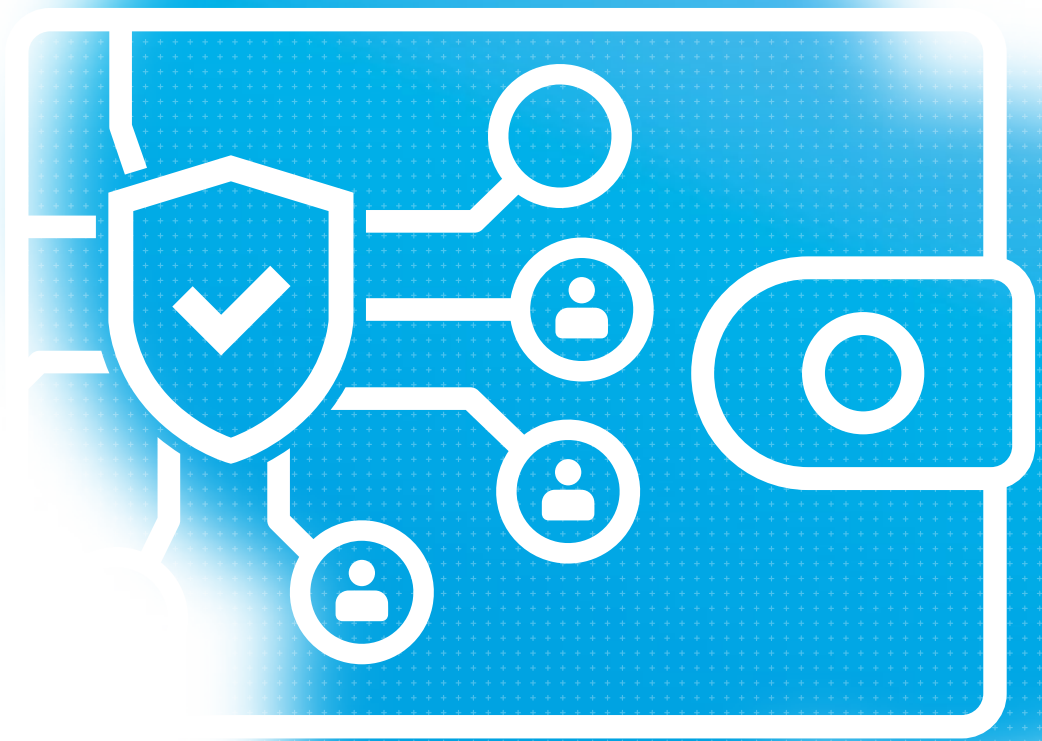
SECURE IDENTITY ALLIANCE

On the road to User-Centricity: Digital Identity in the Electronic Wallet era

An SIA guide exploring usages, policies, models and best practices

2022 Edition



Mentions

Secure Identity Alliance (SIA)

Secure Identity Alliance (SIA) is a global non-profit association representing actors and organisations and adjacent industries active across the digital identity ecosystem. SIA's mission is to unify the ecosystem of identity and unlock the full power of identity so that people, economy, and society thrive. The association supports the development of the activities of its members across four broad pillars: Identity for Good, Outreach, Open Standards Development and Industry Services and Solutions.

www.secureidentityalliance.org

Design

Design Motive Ltd

Photo credits

Shutterstock

Editorial review

Slingshot Communications

We would like to thank the many contributors to this paper.

Production

This report has been produced by the **Digital Identity Working Group of the Secure Identity Alliance (SIA)**

Members of the SIA Digital Identity Working Group:

Kristel Teyras
Thales (Chair of the Working Group)

Guy de Felcourt
Public Affairs Consultant – Digital Society & Identities (Lead Author)

Marie-Sophie Bellot
Pavlina Navratilova
IDEMIA

Calum Bunney
INGroupe

Michael Edwards
Veridos

Paola Heudebert
Steve Lourdessamy
Archipels

Eric Piroux
Entrust

Lanre Ogungbe
Tolu Adetuyi
Identity Pass

Sebastien Zehetbauer
Youniqx (OSD)

John Erik Setsaas
Signicat

Mikel Sánchez Yoldi
Veridas

SECURE IDENTITY ALLIANCE

Contents

Executive summary

The COVID-19 pandemic accelerated the adoption of mobile digital identity tools within e-wallets that enable individuals to use their mobile phones for several purposes including identification, authentication, authorisation.

In this paper, we explore how digital certificates on mobile phones are converging with functional - or so called derived digital identities - and how this is driving the creation of new digital identity policies, regulations and technical specifications that are designed to protect the security and privacy of users and the wider digital ecosystem.

Examining some of the many use cases driving digital identity wallet adoption around the globe, we highlight the key architecture trends, standards and data models that need to be considered when implementing e-wallets for functional digital identity.

Providing a detailed overview of digital identity and best practice pathways in the era of e-wallets, this paper will prove informative for a variety of audiences, including:

- National governments that use functional digital identity programs for digital governance (for example, serving citizens abroad or within national boundaries) and public administration.
- Public service bodies – including health, transport, finance, education, employment, social benefits, taxation, and emergency/rescue that use digital identity credentials to deliver services.
- End User Private Companies – including banks and financial services, insurance, energy, telco, utilities.
- Inter-governmental and non-governmental organisations (IGOs and NGOs) – especially those dealing with migrant or displaced populations.

1.
Section 1.

Introduction

In this section, we look at the evolution of digital identity wallets and how mobile-based digital identity is ushering in a new generation of methods to identify, authenticate and authorise/consent or the exchange of trusted attributes.

In this section you will:

- Learn about the foundational and functional concepts underpinning digital identity.
- Discover the key concepts behind electronic wallets, digital identity wallets, and mobile-based digital identity.
- Explore what is driving the increasingly sophisticated use of mobile-based digital identity and electronic wallets worldwide.
- Discover some of the major policy trends relating to electronic wallets, the mobile management of electronic wallets and how these translate into regulations in regions around the globe.

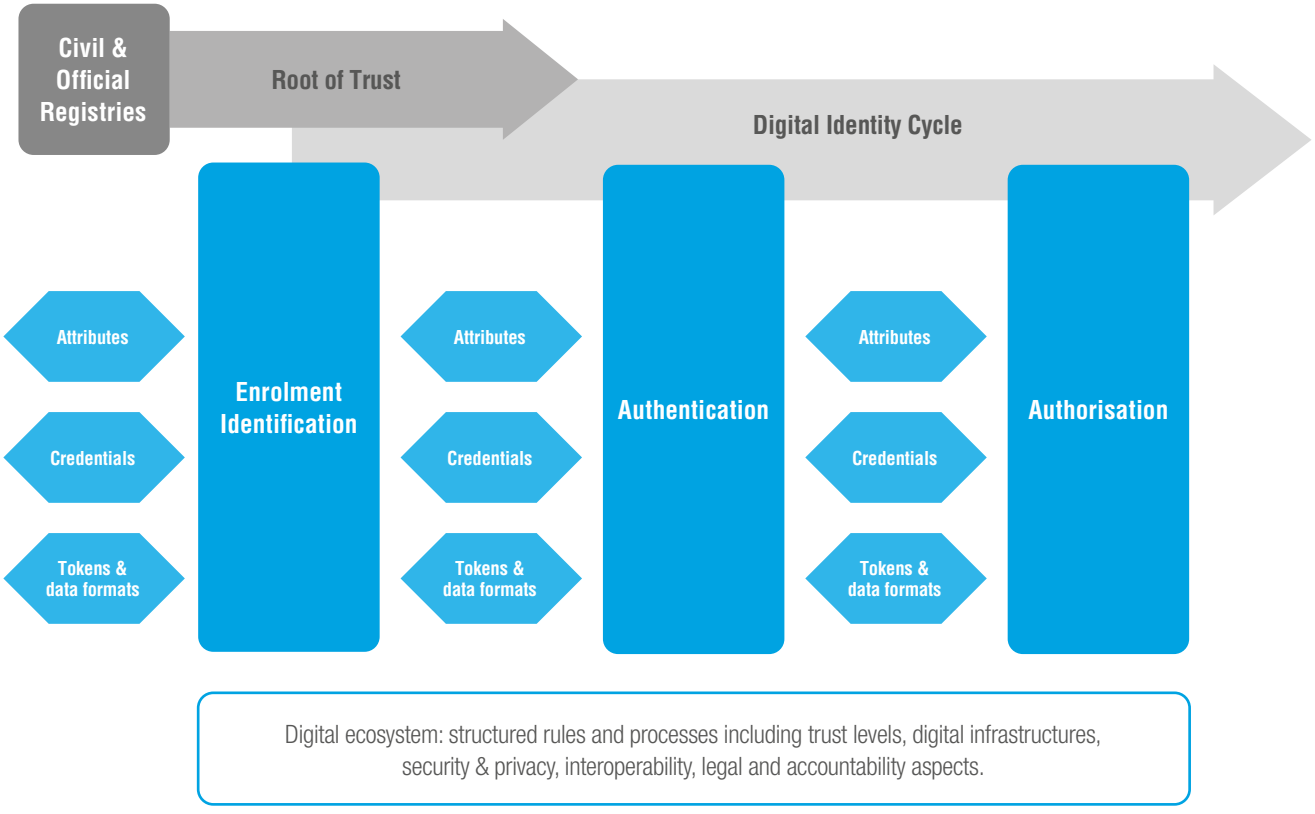
1.1. What is digital identity?

Identity is a set of attributes [REF1] relating to an entity/person that give a singular and meaningful representation of it in each situation or context, for a certain purpose. Digital identity is the utilisation of these attributes to enable people or entities to engage in social and economic interactions. All electronic transactions and digital relationships are enabled by three foundational pillars.

The first pillar consists of **enrolment and identification** [REF2], the second is **user authentication** (usually through checking credentials issued at the identification phase) and the third is **user authorisation**. This last pillar features an exchange of consent (often through digital signatures) and rights management (often through the exchange and/or attestation of attributes).

Digital identity is the organisation and inter-relationships of these three pillars using several instruments as attributes or credentials, along with processing techniques such as cryptography, data management, or biometry. It is a highly structured digital ecosystem that contains rules, processes, and digital infrastructure.

The three functional pillars & cycle of digital identity



1.1.1
Digital identity in the context of everyday life

Whether in the physical world or online, there are four basic reasons for using a digital identity:

Signing up for a new service

When digital identity is used to sign up for a new service, the service provider receives validated information (the individual is who they say they are) while the user experiences a simpler onboarding process. However, some service providers (for example banks) may require additional proof of identity, or proof that the user is "de facto" present, due to regulatory requirements.

The advantage for the user is simpler onboarding. The advantage for the service provider is less friction during onboarding, and higher conversion, as well as getting already validated information.

Gaining access to a resource or a personal account

Digital identity can be used to give the user access to resources, typically by logging in to the services the user signed up for in the previous step. The advantage for the user is the familiarity with using the same credential for multiple services. The advantage for the service provider is not having to deal with the basics of identity (such as account recovery) and reducing the GDPR risk of storing identity data.

Making a commitment, undertaking a transaction or signing a document

Commitments are typically contractual arrangements or financial/commercial transactions. In this case, it is important to know the identity of the individual, as they will be accountable for the transaction or contract.

An electronic signature is typically used in this case and may be used as proof of identity and formal agreement. The user can then be held accountable for the contract, without having to provide additional proof of identity.

Asserting rights and duties or proving something about you

There are several frequent use cases for digital identity, including proving you:

- Are eligible to buy a product (for example, you are of legal age to buy alcohol)
- Are allowed to drive a car (you have a driving license)
- Are eligible for a rebate on public transportation (due to disability or age)
- Have been vaccinated

While a typical situation in the physical world involves presenting an identity document or token (such as a keycard to access a door), the digital world is more complex but also offers more possibilities. For example, a digital identity is a way of proving one, or several of the above using digital means. During the digital identity onboarding process, a user's identity is validated and the strength of this validation determines the user's level of assurance; different providers of digital identity may provide different levels of assurance.

In addition, the user is issued credentials to prove that this is their own digital identity. Usually there are a combination of authentication factors (multi-factor authentication) to enable credential acknowledgment and trusted validation [REF3]. The strength of this authentication also determines the level of assurance for any given use case.

The user can now reuse their digital identity credentials for multiple purposes, without having to go through the identification process every time; only authentication and authorisation will be needed. Let's look at how this works in some real-world scenarios.

In the physical world, each of these scenarios requires you to identify yourself. But in doing so, you will often reveal more information than is required by the verifier.

Using a digital identity, however, makes it possible to limit the information revealed. So you can prove you are eligible for a discount on public transportation, without revealing how old you are, or that you have a medical condition.

1.1.2
Deriving functional digital identity from foundational identity

Foundational and functional identities are different. **Foundational identity** is assigned by the state and given to a person at birth. It enforces the legal status, as well as the rights and obligations of the natural person. The process is similar for legal persons. Identity information is registered in civil registries (or commercial registries for legal persons) and evolves with the different events of the life of a natural or a legal person.

A foundational identity is about documenting the start of this process, and in most nation states it relates to giving that identity a legal status. The idea of status is aligned with national legal systems and may follow guidelines set out by the United Nations. This is the reason why foundational identity is also known as "legal" or "official" identity.

A **functional identity** considers only the relevant information needed to comply with the objectives of a social, civil, or commercial relationship. For instance, a social relationship may only need a name and a sense of age, while a commercial transaction needs a name, an address as an attribute, and a valid payment method.

Functional identities are set for a given situation/purpose and are sometimes known as contextual identities. These can be linked or derived from an official or foundational identity, and benefit from the sovereign root of trust, but this is not always the case. For example, some functional identities do not need any linkage, only a declarative account, with no attestation of an attribute or reduced to few attributes as a valid payment. However, we can say that today most service-purpose personal accounts are based on functional digital identities.

Some countries use a NIN (National Identification Number), which is a unique persistent identifier given at birth. This is an important part of the foundational identity and simplifies ensuring "one user, one identity".

Countries without a NIN use an UID (User IDentifier), which is unique within a given scope, but not persistent, and may change over the lifetime of the identity. As well as making it more difficult to ensure every individual has only one identity, this also allows for synthetic identities (for example, fraudsters creating an identity for a person who does not exist in real life).

For privacy enhancement, there are options such as the use of decentralised identifiers (DIDs). These unique identifiers may remain under the control of their respective users or they may be 'session-only' unique identifiers which cannot be used outside the technical domain.

1.1.3
The need for a trust anchor

Having analysed the proposed user service, an important and recurrent question for the functional identities that are used is how much should these refer to, or be derived from, a foundational identity?

When digital identity relates to our legal or civic identity responsibilities for such things as online tax declarations, then digital services will require a combination of two things: firstly, assurance that the identity has a sufficient foundation in facts, and secondly, that the person presenting these facts as their identity can prove ownership.

Foundational identity does offer one starting point to anchor this need for greater assurance and trust. Its main purpose is to create or help establish a civil or legal identity, which is often bound to official registries and a unique identification number. To harden this foundational process and determine the uniqueness of the person, a biometric method may also be used. However, biometrics are difficult to scale or use in the wider proof of a foundational identity, and the discussion quickly moves to the use of digital authentication methods instead.

A biometric may then be associated or 'bound' to a person's legal identifier, allowing it to be used again to authenticate foundational identity ownership. This is key for proving a user is actually present, and that somebody else is not using the identity. In some systems, almost all service transactions go back directly to this foundational identity – for example, India's Aadhaar solution works primarily in this centralised way.

1.1.4
The next step: derived functional identities

An alternative approach is to view foundational identity, where it exists and is adequate, as the first step to issuing an independent digital identity. New digital identities created in this way may 'reuse' information (known as attributes) about the foundational identity, or create a completely new identity based on a new identifier and set of attributes that relate to specifically to the system the new digital identity has been created for. Known as derived identities, these valid identity credentials are created and maintained using the previous verification of official identity credentials which are bound to the foundational identity.

Well-established examples of this can be found in banking. A bank will check your foundational (e.g., national) identity before giving you a bank identity along with the means of proving that this is your identity (e.g., card + PIN code, or account + digital authenticator). The bank may use your name attribute from your foundational identity. Similarly, a Digital Service Provider may register you directly to establish who you are, trusting you to authenticate yourself correctly using whatever digital authentication method it gives you. In this way, digital identities can be created with confidence from foundational identities, without necessarily using the foundational identity, or indeed its biometric proof.

In summary, a foundational identity based on official registries and using unique identifiers (NINs or UIDs) offers a clear and simple reference model to make that identity widely useful in building a digital identity world. It offers governments the easiest reference point on which to build connected information (attributes) in a sovereign-based approach to identities. UIDs remove the ambiguity or confusion around which physical or legal person is being referred to.

1.1.5
Adoption, choice and ownership

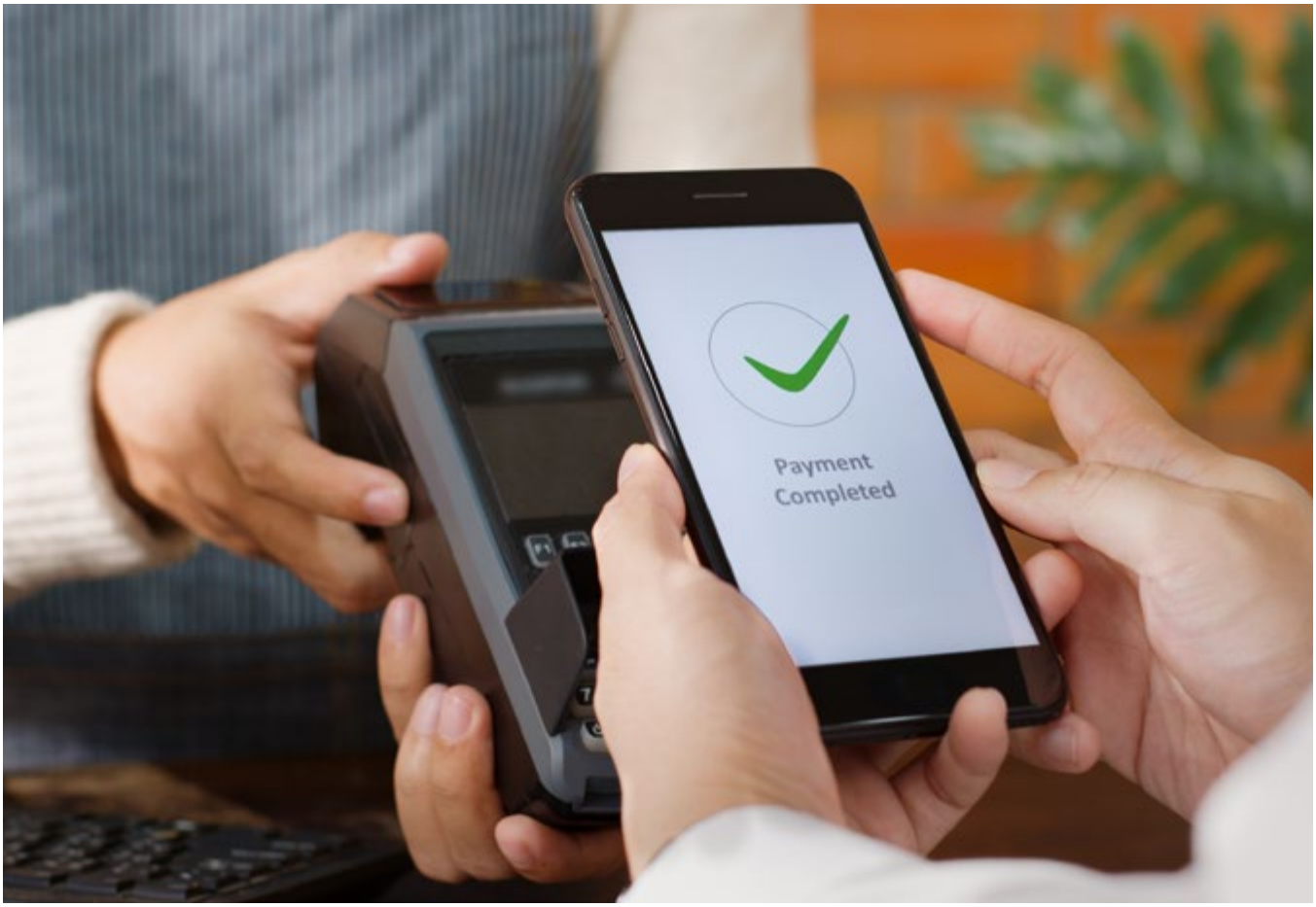
In most countries, users have minimal opportunities to make modifications to information connected to their foundational identity, as this contains legal information. The data is typically limited to NIN/UID, Name, Date of Birth and family relations. In essence, foundational identity is something you have little control over, and attributes are assigned to you.

Your functional digital identity, however, is one you may (largely) choose and build yourself. You choose which parties you are in a relationship with, and own important rights in relation to creating, using, or modifying your data as it relates to your functional digital identity.

1.1.6
Mobile-based digital identity

A mobile-based digital identity encompasses all functional digital identity usage and covers users in either a remote mode (online) or a presential mode (online or offline). In other words, mobile-based identity is primarily a form factor for accessing/managing core functions supported by digital identity: identification and enrolment, authentication, authorisation, and the exchange of information/consents.

Increasingly, mobile devices have become the option of choice for users looking to interface with remote digital or in-presence services and today there are a variety of mobile-based digital identities that can be accessed and managed through smartphones or mobile devices. Formats include **electronic wallets** and **digital identity wallets, mobile applications** used for identification and authentication purposes, digital formats or data models for derived identities or credentials managed on mobiles under the form of attestations of attributes or visible **digital seals**.



The cloud, in conjunction with the mobile environment, allows for a wide combination of data management practices and a simplified user experience. As a result, using mobile-based digital identities as a universal media for delivering greater user-centric convenience now has widespread global appeal. Plus, mobile phones are becoming a universal management tool for handling instant payment electronic wallets, biometric-electronic KYC (Know-Your-Customer), or sanitary credentials.

However, there are some constraints that need to be overcome. These include specific data models, connectivity security and privacy restrictions, interfaces, and interoperability characteristics relating to the mobile phone environment.
As hype about mobile electronic wallets can be confusing, it is important to understand that electronic wallets (including digital identity wallets) can be accessed and managed from media or devices other than mobile phones.
In a similar way, it should be recognised that digital identity is not restricted to mobile-based digital identity alone.

1960-2030: the emergence and development of digital identities

1960	Starting with first computers using login and passwords
1970	Remote login/VPN
1975	Public Key Cryptography allowing individual keys for each entity
1980	User names/NINs/unique identifiers/user name on the internet (reusable)
1990	First Public PKIs emerging and digital certificates
1991	World Wide Web
1995	Public PKIs are emerging
1997	Identity & Access Management emerging into organisations
1999	Digital Signature Directive in Europe
2000-2002	First governmental digital identity credentials for populations, including Estonia as a pioneering successful model
2002-2005	First identity & authentication protocols on the Web: SAML, OPEN ID, FIDO
2003	Issuing electronic identities especially Bank identity in Sweden, a primer for private issued functional digital identity
2014	ID4D - Identity for Development Initiative by the World Bank
2015	Bigtechs (Facebook/Google) sign-up/log-in
2106-2017	PSD2 leverages API for Open Banking and Strong Customer Authentication
2019	Open Standards Identity APIs (OSIA) launched for foundational identity systems interoperability
2021	SSI, electronic wallets and proposal for a Unified European Framework for Digital Identity in Europe (eIDAS/2)
2022	Digital identity wallets
2022-2025	(projection) Strengthening of digital ecosystems around digital identities
2025-2030	(projection) International trust frameworks implementations with mutual recognition for functional digital identities
2025-2030	(projection) International use case implementations in transport, health, digital money and more services

1.2. The rise of electronic wallets

Electronic or digital wallets are structured accounts of data that are usually managed and stored in the cloud (or sometimes directly on the mobile) and manageable and accessible in a secure way from a device. They can run as applications for multiple different usages including payment, identity, health, transport, or other sensitive services, including digital money.

In summary, electronic or digital wallets are a mobile solution that enables citizens to store, manage and selectively disclose identity-related data from different sources and for different purposes. Electronic wallets work can also work in a face-to-face or presentational mode (through NFC or BLE or other communication protocols) or in an online mode using specific mobile applications found in digital marketplaces.

While electronic wallets have been around for several years (electronic wallets were first proposed around 2004-2005), in recent years the growing use of mobile credentials in payment, transportation, and for the presentation of COVID-related health certificates in the form of a QR code or vaccination wallet, means they have truly taken off. Added to which new data models - such as verifiable credentials or the attestation of attributes - now allow for the selective disclosure of specific attributes. Which means users can select the data they need to use to access specific services, and deliver this trusted data in a structured format.

In many countries, the use of digital wallets is growing rapidly, especially for payment. This is especially true in Asia (China, India, others) but is also increasingly so in the US, Australia, Africa, and the rest of the world. Indeed, industry analysts expect half the world's population will be using digital wallets by 2025 [REF4] and that the majority (52.5%) of online transactions (e-commerce) [REF5] will be conducted using digital wallets.

Today's rapid electronic wallet adoption is being fuelled by several key user benefits including the combination of online and offline modes, easy and ergonomic use, ability to keeping track of services used, tickets bought, and transactions made, loyalty rewards, some international interoperability, as well as potential additional privacy, and security features.

Fuelled by the rise of mobile payments, portable biometrics, and QR code attestations related to sanitary conditions, electronic wallets are now over taking payment and transport/mobility use cases to take a leading share in user consolidated behaviour.

1.2.1
Digital Identity Wallets (DIWs)

The primary focus of digital identity wallets (DIWs) is trust usage; identification, authentication, and authorisation usages are all made possible by accessing identity information under the form of attestations of attributes (for example date of birth or a specific entitlement) and official documents (driving license, passport, university diploma, a medical prescription or a transport ticket) that are related to the personal identity under a digital secure format.

In this way, DIWs provide a unified location for digitalised *identity attributes*, *documents* and *certificates*; these pieces of information may be related to *civil-certified identity* attributes or to more independent *functional/commercial personal data*. They also put control of identity more firmly in the hands of the individual, who can choose how much information to share. For example, using a DIW, a user can prove they are over 18 years old without having to disclose their date of birth, address, or other personal data that is typically visible on physical identity documents.

The shift towards DIWs is so significant that the industry analyst Gartner has positioned 'Identity Wallets for Citizens' at the peak of its *Hype Cycle Wave for Digital Government Technology in 2021*. In Europe, the EU-wide *Digital Identity Wallet* project is the center piece of an ambitious unified framework for digital identity [REF6].

There are several important characteristics that need to be considered in relation to electronic wallets:

- **Security and trusted environment requirements** - these are vital for several domains, including identity, payment and health.
- **Multi-purpose vs. restricted wallet** – a multi-purpose wallet could be used for payments, digital money and identification. Meanwhile, a more limited multi-purpose DIW could be used to present attributes and credentials for functional requirements during Know Your Customer (KYC) or Know Your Supplier (KYS) processes.
- **Online vs Offline mode** – sometimes functionality is limited in offline mode.
- **Open or Closed mode** – it is possible to limit the number of parties that can be accessed/served by the DIW. These limitations can be imposed by the ecosystem using different criteria such as trust level, connectivity, previous registration of the service/user, and so on.

Governments and leading retail service providers will need to pay attention to how they adapt current digital identity ecosystems when integrating electronic wallets for citizen and consumer use. Managing identity and data on cloud infrastructures and mobile phones means new security, sovereignty and privacy issues will need to be addressed prior to adoption.

New environmental factors that are driving digital identity policies and regulations

The roads to build a digital wallet strategy and the consequences on the intermediations between services and users must not be underestimated. Typically, three types of organisation are looking to utilise wallets for the delivery of functional digital identity to users:

Government-driven (eg. EU Approach)

Governments can build solutions based on standards and industry offerings, integrating these with their own digital ecosystems and assuring compatibility and interoperability with other developed solutions.

National Private Sector (eg. Banks, Retail)

End-users private firm services can use customised digital identity wallet solutions to develop best-in-class user experiences integrated with KYC, payments, and other key mobile based services.

OEM (eg. Apple, Google)

There are many OEM payment apps, the most common of which are leveraged by big tech or mobile operators. OEMs enable issuers to be present in the pre-installed OEM apps/wallets, allowing their users to perform payments or travel pass checks. Most started in the mobile payment market and are now positioning with identity wallet offerings.

When building digital wallet services, it will be important to consider beforehand who will provide the wallet infrastructure and digital services and to assess the potential consequences resulting from intermediations between services and users.

1.3. Mobile-based digital identity and wallets: global trends and evolutions

1.3.1
Digital identity: a rapid evolution spurred by the COVID-19 pandemic

If we look at the digital identity schemes deployed by governments around the world, it's safe to say that these were initially driven by three common goals: driving inclusion in civil society and digital education (protecting citizen identities and privacy rights); delivering public services more efficiently (and supporting economic growth by making transactions smoother and more secure); and enabling digital trust (contributing to cybersecurity, fighting against online identity fraud, and developing new forms of electronic exchange).

To achieve these goals, many governments have put a trusted digital identity into the hands of citizens, providing a combination of credentials forms - chip cards, software tokens, and secure mobile identity applications – that enable citizens to authenticate themselves, access online public services, and prove who they are during the KYC onboarding process with private service providers.

However, in 2020 the emergence of COVID-19 had a dramatic impact on virtually every aspect of daily life and highlighted, for governments, some serious vulnerabilities where service continuity and resilience were concerned – and made fixing them a priority. The rapid overnight shift away from physical, face-to-face transactions also supercharged demand for trusted mobile identities.

As a result, governments are now accelerating the move to mobile digital identity. According to ABI Research, mobile identity is set to grow at a CAGR of 22% until 2026. Meanwhile, in its 2021 Hype Cycle for Digital Government Technology report, Gartner predicts that by 2023 over 60% of governments will have tripled citizen digital services.

Looking more closely at recent government digital identity initiatives, we can see that the functional requirements for digital identity are also expanding significantly. Going well beyond simply offering citizens an online authentication tool, these now include a wide range of digital identity-related functions in onboarding, authentication, and authorisation policies and practice.

Digital Identity is being redesigned, thanks to the specific user experience and digital wallet features that impact all its core functions: Onboarding, Authentication and Authorisation based on digital signatures, rights management, and trusted attribute presentations.

POLICY AIM 2010-2020	FOCUS ON DIGITAL IDENTITY	TECHNOLOGY EXAMPLE	LEGAL EXAMPLE
Public services efficiency	• Adoption, user experience, comfort of use	• Biometric authentication • Software tokens	• 2014 European Union eIDA • 2016 India Aadhaar
Driving citizen and user inclusion	• Digital literacy • Legal identity for all	• Mobile apps	• 2014 Estonia e-residency • 2015 UN Sustainable Goals 16-9: Legal Identity for All including birth registration
Developing general trust in a digital environment	• Security and cybersecurity • Privacy and user control	• Strong credentials • Multifactor Authentication	• 2016 European Union GDPR

1.3.2
Top shifts driving today's digital identity evolution

The world is changing fast, bringing with it new consumer needs and a modern digital identity can deliver much more than authentication alone. The pandemic created a strong need for enrolment and identification in distance mode. Plus, electronic KYC also is much more demanding on identity and requires a huge amount of flexibility to be able to prove one person's full identity or specific elements of it, such as their age, address, and electronic attestations of attributes. It can be an entitlements attribute (the right to drive or to vote) or it can be a status-related attribute (a student proving university credentials or economic solvency). What's more, citizens want to use their digital identity in the physical world too.

Meanwhile, digital accountability is becoming increasingly important and there is now a stronger push to a more granular form of trust. As the digital environment becomes, by default, the space in which society operates, the need for individual and collective accountability is growing.

Finally, demand for cross-border capabilities is growing and momentum is particularly strong in countries with several states. In the globalised, digital world, there are no borders. As a result, there is a compelling need for citizens' digital identities to be recognized and accepted in other federal states, and abroad.

ENVIRONMENTAL FACTORS	NEW POLICIES DEVELOPED	APPLICATION MODELS	EXAMPLES
Data sovereignty	• Strategic Autonomy for data processing and storage capacity	• Encrypting data for transmission and storage • Server geographic localisation	• Gaia X – European Sovereign Cloud project • Rules for using specific data (eg. health data)
Mobility becomes paramount	• Anywhere anytime access • Permanent connectivity	• Identification authentication and authorisation/consent	• Low Earth Orbits satellites constellation • Wi-Fi 6-7 generations
Electronic KYC and recurrent due diligence	• Electronic KYC and remote identification • Recurrent AML checks or due diligence benefit from being trusted by digital identities	• Remote onboarding with liveness detection and authenticity checks on trusted digital identity • Digital corporate accounts with trusted digital identities	• New EU AML regulation package proposed 2021 for 2024 • International sanctions and embargoes – respect by suppliers
Digital literacy and inclusion	• Digital inclusion for elderly people • Small business entities	• Use digital identity to enable secure and convenient access to digital services • Help small businesses interact online	• LEI as a new legal identifier for corporate transactions on international markets
Cloud-based and identity as a service	• Growing public services on the cloud • Device identities in the cloud	• Corporate and administration staff IAM • IOT identities	
Enhanced privacy requirements	• Implementation of privacy by design • User centricity	• Consent management • Self-sovereign identity • Verifiable credentials	• Selective disclosure of attributes • Zero-knowledge proofs (ZKP)
Convenience and do-not-disturb	• User experience (UX) as a primary requisite	• Streamlined and frictionless processes • User convenience at hand	• Silent authentication • Passive liveness detection • Biometrics and AI
Cross border interoperability	• New quest for functional identity cross border interoperability	• Sanitary and COVID-19 travel pass	• Electronic wallet interoperability • GAIN project
Situational and contextual intelligence	• Increase granularity in risk and trust management	• Dynamic digital identity	• Pattern analysis for event and behaviour detection (ML/AI)
Cross-Sectorial Convergence	• Promote readiness, flexibility, and integration	• Payments, money and identity • Public sector services	• Electronic wallet common architecture • Integration capabilities

1.3.3
Key trends

Since 2020, SIA has observed the following key digital identity trends:

Trend 1: Assuring a higher degree of data sovereignty

Sovereignty has become an important focus of the digitalisation debate. Public services rely on the cloud, so issues of data sovereignty are a top consideration for governments. This means working closely with service providers to ensure transparency, control, choice, and autonomy over the strategic landscape and IT assets such as data, systems, and critical software. Benefits include security, regulatory compliance, and the building of trust with citizens and other stakeholders.

Several sovereign cloud initiatives have taken place since 2020. In the EU, the Gaia X platform is being used to reduce the dependency of European companies and governments on US technology providers and strengthen data sovereignty in the region. In addition to utilising a federated European data infrastructure the initiative features a blockchain and a digital wallet belonging to the user that contains the digital keys for service authentication.

Trend 2: Mobile devices are all pervasive

Mobile devices have become a fixture of modern life, enabling consumers to pay bills, shop, bank, access healthcare services and more. Providing unprecedented levels of convenience, citizen expectations for streamlined digital and mobile experiences are pushing governments to embrace digital transformation as fully as their constituents and commercial enterprises have.

As a result, governments around the world now unanimously view smartphones as a compelling proposition for providing citizens and residents with a secure and convenient digital identity. Especially as the price of a smartphone, the primary entry point for access to the internet in many emerging markets, fell by 30 percent in Asia, about 25 percent in Latin America and the Caribbean, and about 20 percent in Africa from 2008 to 2016. Helping to make the technology needed to expand digital identity even more affordable in every part of the world.

Added to which, the need for trusted mobile identity authentication services worldwide is growing as government bodies look to respond to rising levels of digital fraud. Indeed, according to the latest Research and Markets report, the global market for Mobile Identity Management estimated at US$32.4 billion in 2020 is projected to reach US$54 Billion by 2027, growing at a CAGR of 7.6% over the period 2020-2027.

In parallel, the shift to digital services using identification, authentication, and authorisation logic is set to go yet further as additional connection fluidity (5G, Low Earth Orbit Satellites, Wi-Fi 6-7 generations) generates permanent access to essential services at any time/anywhere in the world.

Trend 3: Electronic Know Your Customer (KYC)

The need to onboard massive numbers of users or customers in a remote digital way has also impacted the KYC practices and increased the synergy with digital identity practices. Electronic KYC has been the route of choice for public administrations and the regulated private sector. While KYC starts with customer or user identity, electronic KYC starts with digital identity for enrolment.

KYC practices for natural and legal persons have, to date, been focused on business-related customer information relating to risk and solvency. However, KYC practices are transforming to encompass a much larger volume of data and financial/corporate size companies now need to check and analyse a wide range of economic, social, and ecological impact information on their suppliers and customers. They also need to demonstrate/prove that they are respecting international sanctions and embargoes in relation to certain geographic zones or specific entities. This may also include anti-corruption practices and extraterritorial compliance.

In addition, new KYC regulations (for instance the European Union's AML Package presented in 2021) are extending the scope and depth of the AML rulebook. This includes risk assessment monitoring, vigilance obligations, whistleblowing procedure, and recurrent KYC checks.

Digital identity is therefore not only the new entry point into remote KYC onboarding but also the trust anchor for the business relationship, the recurrent checks on compliance, and periodic due diligence when required.

Trend 4: From inclusion to in-depth inclusion

There has been significant progress in achieving the United Nations goal to give every person living on the planet a legal/official identity by 2030. Since 2020, however, new inclusion challenges have arisen in relation to mobile-based digital identities. Primarily these relate to digital literacy: teaching people how to access services in the digital world, manage their accounts, detect malicious phishing messages, and interact in an appropriate and amenable way with each other. These needs range from coaching (to emancipate digitally) to digital guardianships (help or support for elderly people for instance).

Other inclusion programs are focused on responding to the identification and authentication needs of businesses and organisations when interacting with one another. Digital identity provides a secure means to verify company identity and engage proportionate accountability for a given business or organisation.

Trend 5: The rise of cloud-powered managed services

COVID-19 boosted demand for managed services as businesses and the public sector embraced easy-to-scale cloud services. According to Fortune Business Insights™, the global managed services market size is expected to hit USD 557.10 billion by 2028 while exhibiting an impressive CAGR of 12.6% between 2021 to 2028. The increasing adoption of cloud-based managed security services is also fuelling this market growth.

Similarly, digital identity as a service delivered through the cloud is also rapidly growing in the wake of Identity Access Management (IAM) and identity for the Internet of Things (IoT) and infrastructures, and is now reaching more public services. New trends in this space include contextual security such as Zero Trust, Cloud Security and Response (CSR), and User and Entity Behaviour Analytics (UEBA), all of which are contributing to the development of cloud-based identity services articulated with devices and mobile phones.

Trend 6: Privacy requirements become more stringent

Privacy concerns have grown with the rise of social platforms and networks. Despite better regulations protecting users, citizens, and consumers worldwide, the situation remains critical in many regions of the world. For instance, in the US, more than 90% of Americans believe they have lost control of how their data is collected and used by all sorts of entities [REF7]. This is a natural response as according to the barometer of the International Cybersecurity Forum 2021, data breaches are constantly on the rise: in a year and a half, the number of data breaches per day has increased from 4.5 to 7 [REF8].

As a result, the need for privacy-enhancing technology that goes beyond data minimisation principles to truly implement privacy by design has become stronger. The concepts of user-centricity and consent management play a central role in new digital identity implementations. This trend is also accompanied by an explosion in the number of companies specialising in privacy tech. Data protection authorities are also incentivising innovative privacy-enhancing research projects [REF9].

Two recent notable and related developments - selective disclosure and Zero-Knowledge Proof (ZKP) – are fundamental for Digital identity or attribute models such as self-sovereign identity and its verifiable credentials, as these make it possible to prove information without disclosing the questioned data.

- **Selective disclosure** allows an individual to share parts of a larger data set. For example, a user wishing to access an online sports betting site does not have to disclose or display his address on his digital identity to prove that he is over 18 years old; he/she simply shares his/her date of birth. The proposed EU Identity Framework Regulation [REF10] requires that digital identity portfolios technically allow for the selective disclosure of individuals' attributes [REF11].
- **Zero-Knowledge Proof (ZKP)** is a cryptographic security protocol that makes it possible to prove the authenticity of an attribute about an individual without having to reveal the value of the data - demonstrating that a set of attributes satisfy certain characteristics without disclosing the value of all these attributes. So, an individual wishing to access a sports betting site can only reveal the assertion they are over 18 years old without revealing their precise age. ZKP protocols are among the most protective in the world when it comes to protecting the privacy of users of online services and guarantee a significant limitation on the use of personal identity attributes by going well beyond the principle of data minimisation, which is difficult to respect in practice. The European Parliament has already recognised the potential of the ZKP to resolve the conflict between data minimisation and multi-party data verifiability.

Trend 7: User demand for convenience and 'do-not-disturb' ergonomics

There used to be an inverse relationship between online security and end-user convenience. When you tightened security, it used to mean more hoops for users to jump through and more 'sign-ons' to endure. But with end-users becoming more demanding when it comes to convenience and intelligent security mechanisms, user experience (UX) and UX design have become primary requisites for functional digital identities and especially for mobile-based digital identities.

Users are searching for trusted, fluid, and personalised services to help them navigate their way through an increasingly connected and digital world. New options appear to allow time or geographic zones to escape from permanent connectivity notifications, with parameters that allow for the deactivation of what is not considered as high priority messages, services, or tasks.

Effective solutions need to be secure enough to protect digital identities, while seamless enough that consumers will want to use them. Fortunately, various techniques – including biometry, artificial intelligence (AI), silent authentication, and passive liveness detection - now provide streamlined and frictionless solutions that strike this balance between security and convenience.

- Using **biometrics** as a means of authentication and verification is now mainstream and frequently utilised by both public and private identity schemes as a reliable, hassle-free process for onboarding, validating, and approving new service users while providing increased assurance to providers that a person is real by verifying a tangible, real-world trait as both something the user has and something the user is. While the internal process for biometric authentication is highly technical, from a user's point of view it's incredibly easy and quick and most people now use biometric verification in their everyday lives: taking a selfie to run face recognition or placing a finger on a scanner to unlock an account in seconds. Convenient and faster than any other authentication method, biometrics also eliminate the common user issue of forgetting a password or a PIN.
- **Artificial Intelligence (AI)** can analyse hundreds of variables to determine unusual patterns that may signal account takeovers. Platforms can use AI to define typical customer behaviours and detect anomalies that stray from the norm in real-time. Abnormal transactions are scored on their likelihood of being fraudulent and can be sent to human agents for further analysis.
- Based on AI, **Silent Authentication** technology uses similar patterns to continuously improve the user experience and deliver more convenience. Also referred to as Continuous Authentication, it was originally designed to deliver convenient and robust risk-based security for online transactions in the banking sector. The mechanism relies on THE continuous monitoring of devices, networks, and user behaviours and is done through standard sensors present in today's smartphones. Enabling the passive identification and authentication of users, it reduces friction/tasks for users, thanks to a powerful and continuous machine learning data analytics to evaluate how you use your phone (behavioural biometrics), your surroundings, geolocation, etc.
- **Passive liveness detection** is a critical part of the digital identity process for face biometric authentication, onboarding, and fraud prevention and is essential for combating identity presentation attacks like photo/video spoofing, deepfakes, models, or 3D masks. Liveness detection can be done in two ways. Passive liveness detection is rapidly gaining market traction because it is more secure and provides a smoother user experience; passive methods typically take a single image that is examined for an array of characteristics to conclude if a live person is present or not without any need for a specific movement or gesture. Active liveness detection expects the user to do something to confirm that they are a live person; change their head position, nod, blink their eyes or follow a mark on their device's screen with their eyes.

Trend 8: Cross border interoperability is the new horizon

The success of national digital identity programmes is reliant on achieving the mass adoption needed to deliver value and secure usage to a complete ecosystem. Global geopolitics factors include geographic mobility, increased regional integration in various parts of the world, economic migration flows nurturing diasporas' digital relationships, and dual nationality's wider adoption.

As the digital world encompasses not only business but also cultural and citizenship relationships, interoperability and standards in digital identity are becoming increasingly important. Governments looking at cross borders movements have made official identity credentials and mutual recognition the first pillar of achieving this interoperability with neighbouring countries and are now exploring ways to digitalise global passports so that passengers can enjoy a seamless travel experience. To achieve this aim, the International Civil Aviation Organization (ICAO) and International Organization for Standardization (ISO) are working with governments and technology experts to define and develop technical specifications for the Digital Travel Credential (DTC).

The need for interoperable COVID-19 vaccine certification and international proof of vaccination status means the cross border interoperability quest for functional identity interoperability is also growing. The EU common format for the digital Covid certificate based on QR code technology is a basic example. Today the European Commission is looking at solutions to enable the use of digital identities across EU Member States. The European digital identity framework will be available to all EU citizens, residents, and businesses in the EU and will enable citizens to prove their identity and share electronic documents held in their European Digital Identity Wallet. The project objective extends way beyond credentials and authentication to encompass several attributes that will require various degrees of attestations and can be used for wider functional purposes (typically enrolment, authentication, and authorisation).

Other initiatives are striving to build a standard-based interoperable system on a still wider worldwide basis. For example, the Global Assured Identity Network (GAIN) program wants to leverage the capacity of financial institutions to offer high-trust identity assurance within a safe and properly regulated environment as means to achieving a major step toward interoperable Digital Trust.

The international interoperability of digital ecosystems is entering a new chapter, thanks to electronic wallet technologies and the enhanced coherence of trust levels. The European Digital Identity Wallet is an example of an initiative looking to achieve trusted international interoperability.

Trend 9: Situational and contextual intelligence closer to identity

In managing trust, government historically used two distinct instruments with two separate boundaries. The first would sit on digital identity and the defined and structured roles, policies, and processes to run the functional needs of identifying and onboarding, acknowledging credentials and authenticating, and running authorisations based on asserted rights and roles of individuals or legal persons. The second used data analytics and AI to detect, categorise and assess risks and opportunities about observed behaviours or events with contextual and situational attributes. The combination of both delivered an optimal combination of risk management and trust capabilities.

SIA has observed several enhancements in adopting situational and contextual intelligence closer to identity. For example, AI detecting events or monitoring interactions can now be integrated into dynamic trust policies around digital identities. Similarly, the integration of multiple situation patterns into machine learning can leverage risk and trust decisions based on functional digital identities into a finer situation and contextual awareness.

Trend 10: Cross-sectorial convergence is strengthening

In the public and private sectors, silos and market interdependency have always been a challenge.

For example, some governments' traditional structures have aligned poorly to address developing global and secure access to their citizens, due to many isolated developments. It has taken some time when implementing national digital identity programs, to consider usages across all ministries and related services to first mutualise cost, and second, ensure adoption. While many national digital systems have collapsed into data silos, more and more nations are now embracing a whole-of-government approach.

When we look at the private sector and functional digital identities usages, we are also observing other cross-sectorial convergence. This is the case for instance between identity and payment and is likely to happen in the future between identity and money, with the development of electronic wallets and Central Bank Digital Currencies (CBDC).

- In the EU, the Payment Services Directive (PSD2) regulation is a good example of the convergence between identity and payments in the digital environment. The European Commission was willing to increase competition and security in the European payment industry and has implemented Strong Customer Authentication (SCA) to ensure electronic payments are performed with multi-factor authentication to increase the security of electronic payments. New developments are being embraced in the payment sector toward identity verification and protection of financial transactions against identity fraud. Payments and other transactions need the support of digital identity in an increasing manner.
- Digital wallets are expected to bring further cross-sectorial convergence. In the traditional mobile application, each sector domain is building its applications for identity, transport, mobility, payment, digital money, etc. It is now expected that the architecture of trusted digital wallets with verifiable and attested attributes, and user choices to use selectively derived official identity or payment instruments, will increase synergies and convergence in using digital services in all situations.

1.4. Case Studies

European Union:

European Digital Identity Wallet

In Europe, the European Commission is proposing to adopt a European Digital Identity Wallet (EUDI Wallet) regulation and architecture framework for storing and managing identity data that would be accepted in all member states and be trustworthy and interoperable. This would facilitate the use of many public and private services, both physically and online, for European citizens.

Target date of implementation
2024

Status
Legislative process – Toolbox and Pilot testing – Development (2022-2023)

Statistics
Up to 400 million potential users (2025-2030)

Strategic objectives
- Strengthen the national electronic identity system under eIDAS
- Improve user control on attributes and credential use through the mobile Wallet
- Allow private sector to develop identity linked services with greater convenience

Technical status
Technically the Commission has been working on specifications organising the functional requirements for online and offline use and the different roles around the EUDI Wallet ecosystem: Users, Issuers, Providers of Identification Data, Providers of Registries, Attestation of Attributes Providers (Qualified and non-Qualified), Certificates for Signatures or Seal providers, authentic sources, relying parties, conformity assessment parties, and supervisory bodies.

User benefits
- Ergonomic convenience in using identity attributes and credentials
- All functional identity pillars in one place: identification, authentication, and authorisation
- Trust levels and attestation of attributes.
- Enhanced user control
- Extended European interoperability

Other Benefits
- May possibly be used with several architecture models: centralised, federated, decentralised

Future developments
- New trust services (remote digital signature, digital archiving, electronic ledgers)
- Cross sectorial use of one functional identity at the choice of the user

Liechtenstein:

Mobile Derived Identity

In April 2020, the Principality of Liechtenstein launched a new mobile-based electronic identity named eID.li and is planning to phase out its smart card in the coming months. The eID.li app is tied to the mobile device that was used for registration through cryptographic measures. Users can then utilise their eID.li app to log in to a service and authenticate by using biometrics. The current ambition of the Office of Information Technology of Liechtenstein is to expand the digital identity scheme to the private sector and become eIDAS notified in the coming years.

Target date of implementation
2020

Status
Running

Statistics
- 40.000 population
- Over 20.000 users
- Over 200 public services

User benefits
- Multifunctional wallet solution
- Protection against identity fraud
- Derived digital identity can be presented through the mobile app

Other benefits
- Easy expandability for future technologies and private sectors
- Easy to issue, update and revoke the digitalised credential
- Providing real-time accurate information
- Mobile document wallet with sanitary credentials (COVID 19)

Future Developments
- The app can be expanded as required to derive other official documents and make them available in a secure way on the mobile phone, similar somehow to a wallet

Austria:

Virtual citizen card

Austria was one of the first European countries to implement a national identity system based on an electronic identity, strongly embedded in the e-government initiative. Austria has a virtual Citizen Card (CC), which can be installed on several devices based on a technology-neutral approach: smartcards or mobile phones. The main objective is to reduce costs and efforts for the government, as well as save time and money for citizens and businesses.

Target date of implementation
2003

Status
Running

Statistics
- 9 million population
- Over 3 million users
- Over 300 public & private service providers

User benefits
- Large multifunctional digital identity
- Digital identity can be presented through the mobile app and Smart Card
- Protection against identity fraud

Other benefits
- Electronic representation: the holder can carry out legal transactions on another person's behalf
- Trusted onboardings with better data quality for service-providers
- Digital signing through always at hand through the app

Future Developments
- Evolution toward European Digital Identity Wallet

Monaco:

Extended Monaco

In the European Principality of Monaco digital identity is now a cornerstone of a major transitional eGovernment program – Extended Monaco. Monaco is a small, but densely populated city-state developing both eGovernment and Smart City service platforms to extend and simplify the way that citizens, businesses, and administrations work together.

The program includes multiple identity technologies – e-ID cards, PKI, biometrics, digital identity wallets – to build an eco-system that is secure, frictionless, and attractive to local people and businesses. Consistent with Monaco's European background these identity components sit alongside a set of trust services packaged for easy use in Monaco's mobile digital application mConnect or using desktop browsers.

The Monaco identity program includes two streams. M-ROAD, which addresses Identity Provider services; and W-ROAD which focuses on digital authorisation and electronic trust service integration. Combining technical components and integration services IN Groupe has led the delivery of this aspect of the Extended Monaco project.

Target date of implementation
June 2021

Status
Running

Statistics
- Solution services the adult part of the resident population of approximately 40,000 people
- Monaco nationals: 25% of population is under administration of the Mairie/Town Hall
- Monaco residents: 75% of population is under administration of the Police
- 5.8% of Monaco GDP comes from the digital economy (2018 figures)
- 3.2% of private sector employment is in the digital economy (2018 figures)

User benefits
- The convenience of a working 'tell the authorities once' eGov interface
- The re-assurance of high security using either a mobile or an electronic identity card method
- The simplicity of access anywhere, anytime using the mConnect mobile digital application or a desktop browser
- User control with explicit procedures for consent and user authorisations
- Securing transparency to individuals of their business with the administration
- Common eGov services delivered as secure, ready to use tools in the mConnect app and eGov gateway
- Self-service identity management options on-line and using self-service kiosks in local offices
- EU compliance for eIDAS identity and trust services, and for GDPR personal data protection

Other benefits
- An open standards solution for long-term stability – OIDC and OSIA
- Federated identity support for commercial stakeholders such as telecoms and utilities
- Establishment of a foundational pillar in growth of the local digital economy
- Introduction of smart phones as a user client platform (mConnect) for many procedures accelerates adoption
- Strong customer service concept of a one-stop-shop for identity, security, and services
- A well-defined and workable digital approach to management of legal citizen consent
- Efficient use of biometrics to support unattended digital identity onboarding procedures

Future Developments
- The Extended Monaco program includes many phases of development. More information is available from https://extendedmonaco.com/en/.

2.
Section 2.

Introduction

In Section I of this paper we explored the evolution of digital identity and some of the key trends and drivers behind the rise of mobile identity and electronic or digital wallets. With digitalisation becoming mainstream for all societal and commercial activities, the use cases for trusted digital identity are exploding and the need for digital trust – using various cybersecurity and identity layers – is becoming paramount.

Digital Identity has now become central to enabling identification, authentication, and authorisation in both the physical and digital worlds in any situation where interoperability (multiple parties), ergonomic (personalised and streamlined trust services), or global security (including privacy) are needed.

Similarly, the mobile-based digital identity environment itself introduces a new generation of methods to identify, authenticate and authorise/consent or exchange trusted attributes and brings identity, KYC, and transaction information to a new streamlined level.

In this Section, we evaluate what stakeholders will need to consider when planning their digital identity programs. After which, we undertake an in-depth evaluation of emerging standards and regulations from around the globe.

Progressively, the world's regions are adopting legislation and key policy rules to structure the digital identity and data landscape into a trusted ecosystem environment. A move that has accelerated since 2020, thanks to the increasingly strategic role played by digital.

2.1. Undertaking a preliminary assessment for digital identity

Because digital identity is now mainstream, a wider assessment of requirements and risk analysis needs to be conducted when assessing the requirements for building customised functional identities for specific services.

A simple methodology, based on five questions, will enable stakeholders to pre-assess these needs from a variety of different perspectives and undertake a risk / opportunity analysis of the intended services or use cases.

By working through this preliminary assessment, stakeholders will be able to clarify project objectives, assess the main risks and best strategies for managing these, determine which trust mechanisms to use, and ensure alignment with the environment (framework) and ecosystem (interoperability, schemes).

a) What are the contextual situations relating to the use of digital identity?

Which situations need to be considered in priority? In which proportion and frequency for an active user? This includes thinking about:

- Physical / "In presence" or nearby situations – will the service use only local connectivity or will portable credentials be needed?
- Digital / Remote / Online services – is online access needed, will this be distant server or cloud-based?
- Virtual /Metaverse / Web3.0 – the use of crypto/blockchain tokens, use case may be in an augmented reality context (gaming, digital art, other).

b) Which digital identity functions will be used when interacting with the service?

Which digital identity ecosystem functions need to be in place for users related to the proposed service /transaction/operation?

- Identification and enrolment (including credential issuance).
- Authentication.
- Authorisation and consent (including digital signatures).
- Attestation of attributes and credentials (declarative, verified, certified by QTSP).
- Others (KYC, transactions, others specific).

c) What is the legal and regulatory framework that is specific and applies to the use case?

In addition to general legal requirements, are there any specific legal/governance/sectorial frameworks that need to be considered for the service. These may differ, depending on whether an organisation is government/administration/public sector or operates within a regulated private sector (AML CFT compliance regime).

Sectorial specific rules may also impact digital identity processes for transport, health, utilities, banking and financial, or Trust service provider.

2.1
Undertaking a preliminary assessment for digital identity (continued)

d) Risk exposure and mitigation measures

How sensitive is the service? What risk mitigation and counter fraud schemes will be needed?

- Trust anchor to official or foundational identity
- Trust level high/substantial for identification and authentication
- Trust level high/substantial for specific attestation of attributes or credentials
- Data analysis with artificial Intelligence and behaviour anonymous data from the user
- Others

e) The exigencies/ level of expectations

What are the top priorities for the use cases being considered, and which priorities will outweigh or have precedence over others (how will these be weighted?). Key issues to consider here will be:

- **Ergonomics:** ease of adoption, the comfort of use, user experience, simplicity of understanding
- **Performance:** service integration, efficiency, productivity, economics
- **Interoperability:** federation, ecosystem, global interoperability
- **Security:** IS security (cloud and on-premises), trust commitment, cyber security
- **Privacy:** user consent, purpose and data minimisation, user control degree, others
- Accountability requirements, trust, and legal validity, internal and external auditability

Stakeholders can build a matrix containing the five entry-point criteria, matching the questions proposed in the methodology and adding a value to differentiate the relevance of each criterion, as shown in the graph below:

Situations coverage

Criteria	Value
Presence	1-3
Remote	1-3
Virtual	1-3

Functional requirements

Criteria	Value
Identification	1-5
Authentication	1-5
Authorisation	1-5
Attestation	1-5

Framework regimes

Criteria	Value
Government & Public	1-5
Regulated AML CFT	1-5
Regulated sectorial	1-5
Other	1-5

Risk prevention

Criteria	Value
Trust anchor & derivation	1-3
Trust level functional	1-3
Trust level attributes	1-3
Other	1-3

Level of exigencies

Criteria	Value
Ergonomics	1-5
Performance	1-5
Security	1-5
Interoperability	1-5
Accountability	1-5
Privacy	1-5

2.2. Policies and regulations

While today's digital identity ecosystems are primarily governed on a national boundary basis, rising cross-sector usage and wider international interoperability are raising the importance of governance forums, sectorial coordination, and regional interoperability for digital identity ecosystems.

In some world regions, this is a strong governance point that is inspiring or building policy orientations and regulations.

- The **EU is the leading example regarding regional level governance evolution that aims to deliver fundamental rights in the digital world and equal opportunities across the Single Market for the various economic stakeholders.** In 2014, the adoption of the EU Regulation on Electronic Identification and Trust Services - eIDAS – defined the European model for trust services as well as trusted digital identity provision. By creating consistent legislation and contributing to better standards across the EU for electronic authentication, eIDAS has also allowed progress in establishing norms and developing infrastructure, looking also to improve cross-border business.

  However, take-up and implementation has been patchy, to say the least. While some institutions in the public sector issue and accept electronic identities from other Member States, many still do not. Acceptance in the private sector of eIDAS notified identity schemes varies from one country to another but has been typically low or non-existent. Today about 60% of the EU population has access to digital identity, but only 14% of public services allow cross-border authentication. Meanwhile, citizens have expressed a desire for greater convenience, with 63% saying they want a single secure digital identity to access services, according to a 2020 Eurobarometer survey.

  The new regulation proposal is looking to be more pragmatic with new measures such as regulated private sector enforcement, the introduction of a digital identity wallet, and the development of new trust services. From 2024, the EU Digital Identity Wallet should become available to every citizen who wishes to use it and public and private sector service providers (such as banks and telcos), will have to accept it as proof of certain personal attributes. From providing electronic signatures to paying fines or accessing health services, EU citizens should be able to use the EU Digital Identity Wallet in every Member State with full mutual recognition, and interoperability, generating millions of authentications every day.

2.2
Policies and regulations
(continued)

- In **Africa, greater regional coordination between states is emerging in relation to the adoption of digital identity policies.** This is the case for instance for the Economic Community of West African States (ECOWAS) [REF12] or the Eastern African Community (EAC) [REF13] which now supports mutual official digital identity recognition based on electronic passport identity, as the first planned step. At the continental level, all states participating in the African Union are also participating in the Smart Africa Trust Alliance (SATA) [REF14]. Smart Africa is an innovative commitment from African Leaders and governments to accelerate sustainable socio-economic development on the continent and enable Africa's participation in the knowledge economy through affordable access to Broadband and usage of ICT. Smart Africa is also running a digital identity program "to establish institutional ownership and accountability, combined with a trust framework based on standards and trust assurance mechanisms to facilitate cross-border interactions." Interoperable digital identities are considered by the Alliance as a strategic tool for boosting intra-African trade as well as physical mobility between member states. The future digital ecosystem aims to promote the movement of people (assisting labor, families, and marginalised groups to cross borders), data (e.g., enabling data pooling and sharing, cross-border credit scoring), money (e.g., accessing bank accounts, enabling cross-border payments) and of goods (e.g., boosting e-commerce, facilitating continental free trade initiatives). Digital identity will therefore form the backbone of Africa's future transformation into a single digital market and the Alliance is bringing together a cross-continental consortium of public and private stakeholders committed to realising a common digital identity certification process. Underpinned by a sustainable framework of agreed principles, procedures, and technical standards, the Alliance has announced it wants to utilise federated governance to build trust among all parties involved in the Alliance, whilst ensuring that the sovereign rules set by member states remain respected.

- Other multilateral or coordination forums are also trailblasing the uptake of digital identity, alignment, and interoperability between countries. The **Digital Government Exchange (DGX)** for instance is an annual global gathering of government Chief Information Officers (CIOs) and public sector leaders from digital governments and smart cities. Today these include Australia, the Netherlands (Amsterdam), Canada, China (Shanghai), Denmark, Estonia, Finland, France, Israel, Japan, New Zealand, Sweden, the UK and the US. In 2020 a working group on digital identity was initiated among some of members to study conditions for mutual recognition and interoperable digital identities and infrastructure and a first progress report has been issued [REF15].

Digital identity governance is also being influenced by global intergovernmental and international standards bodies, and industry organisations which are contributing to the definition of business and technical rules for governance, standardisation, and interoperability.

ISO 18013

The **International Standards Organisation (ISO)** brackets together a wider set of technical standards around different aspects of digital identity that offer to build technical consensus and the means of achieving interoperability for interchange (allowing building blocks to be interchangeable across vendors, whereby preventing vendor-locking). The governance aspect of this is simply a question of adoption on voluntary basis and testing. The list of ISO standards in the digital identity space is growing fast. In parallel with there are other related digital standards from the IETF and from ETSI which may be referenced in the same way, except that they are endorsed by industries and not by National Bodies with generally participation of public authorities on most of the topics bearing on Identity. Accordingly, the ISO standards development process is achieved across several steps subject to decision at National level. Digital driving license technologies is an example requiring coordination on the part of ISO to consolidate what might be expected of an international standard for driver identities.

ICAO DTC

Organisations such as the UN **International Civil Aviation Organization (ICAO)** also contribute. ICAO does not create or publish technical standards like ISO/IETF/ETSI, but it does define how these should be used in the context of international travel document interoperability. It is in part owing to the existence of such a global organisation that this governance coordination role was possible along with standardisation. Digital driving license technologies, on the other hand, may require more coordination on the part of ISO to consolidate what might be expected of an international standard for driver identities.

W3C

Another important market vertical that is influencing the identity sphere is the **Internet**. Lately the 'Internet of Things' has taken the recognition of machine identities to a whole new level. However, the ability of the Internet to manage personal digital identity remains deficient and footprints/privacy continue to be exposed to unknown and dangerous actors willing to use private identity and personal data for damaging purposes. To address this issue, the **Decentralized Identity Foundation** and the **Trust Over IP** initiative have been driving a new set of standards for personal digital identity on the Internet. The W3C set of standards provides a data model for Decentralised Identity management involving Decentralised Identifiers (DID), Verifiable Credentials (VC) and Verifiable Presentations (VP) offering a technical basis to govern digital identity over the Internet in a decentralised approach,and is, with OAuth 2.0 framework based solutions, the technical basis of most online services today. Among the first steps toward global governance using such a technical approach will be international businesses and regional government groups choosing to adopt and endorse such technical approach.

New standards, protocols and data models are emerging in digital identity following the rise of electronic wallets. ISO 18013, ICAO DTC and W3C data model as well as OAuth 2.0 framework for delegation of authorisation are among the most promising ones in this new generation.

2.2
Policies and regulations
(continued)

Digital identity best practices and governance are also evolving in line with sectorial usage evolutions in five key industry sectors: Banking and Finance/Health/Transportation/Public Administration of Social Benefits/Payments.

- **The banking and financial sector** has played a leading role in this field, as attested by the history of the 'smart' chip card. At an industry level, banks in regions such as the Nordics decided some time ago to co-collaborate on the creation of a business model for customer digital identification and authentication. This was made possible by the pre-existence of a clear foundational identity approach to UIDs at a national level which enabled banks to leverage basic attributes and establish new digital identities and means for their customers. The success factor of these schemes has been their critical mass of adoption, leading to a virtuous circle of more connecting services outside of the financial industry. Even Nordic governments now rely heavily on this industry, or commercial sector, methods to authenticate citizen identity.

- The regulated private sector is progressively lying with a high level of governance and compliance in terms of **Know Your Customer (KYC) and Anti-Money Laundering (AML) legislation**. The concept of customer identity-checking has been widespread for some time, mostly using physical identity documents. However, increasingly KYC/AML use digital identity as the source of identity trust and attributes. Indeed, behind many government-driven digital initiatives is the idea that digital identity wallets will support KYC for many business sectors, with the ability to prove identity with high assurance and the capacity to share attributes selectively under the control of the user.

- The **payment industry** is also impacting digital identity policies. Legislation like the **EU Payment Services Directive (PSD2)** has led banks to untie their concepts of customer authentication (proof of who you are) and customer authorisation (proof of what you are allowed to do). Customers can now use their digital identity between different bank services to access accounts and instruct payments. For this to become interoperable, the governance of digital identity authentication was set at a minimum technical level for strong authentication, specifically the means of proving your claimed digital identity.

- Other sectors are entering the digital identity debate but at different rates. For example, the emergence of **digital vaccination certificates as a form of credential** brought with it a national health industry governance mechanism based on a trust layer agreed upon and shared by participating states. The World Health Organization (WHO) has a similar approach to ICAO, in using its own trust and governance approaches.

2.2
Policies and regulations
(continued)

Examples only – not comprehensive list

WORLD REGION	KEY POLICY ORIENTATIONS INCLUDE	REGULATIONS OR POLICY INSTRUMENTS (DECIDED OR PROPOSED)
European Union	• Digital trust services and Identification • Online key digital services with digital identification • Privacy • Data platforms and competition • Practices in the digital world • Unified Identity Framework • Unified AML-KYC framework • Cybersecurity • Payment and open banking • Artificial intelligence, Blockchain, Quantum Computing	• Electronic Identification and Trust Services for Electronic Transactions Regulations (eIDAS) • Single Gateway • GDPR • Digital Market Act • Digital Service Act • eIDAS- EUDIF proposal • AML Package Proposal • UK Digital Identity & Attributes trust framework • Cybersecurity regulation proposal (in alignment with NIS1&2 directive, Cybersecurity Act) • PSDII towards revision or PSDIII
North America	• Privacy • Digital trust services and identification • Data sovereignty and territoriality • Consumer Financial Services • Cybersecurity • Artificial intelligence, Blockchain, Quantum Computing	• US Computer Fraud and Abuse Act • US HIPAA (health) • US Gramm-Leach-Bliley Act • The US Clarifying Lawful Overseas Use of Data Act • US State laws such as California Consumer Privacy Act (CCPA) & Consumer Privacy Rights Act (CPRA) • Canada Personal Information Protection and Electronic Documents Act (PIPEDA) • Canada Directive on Identity Management • Mexico - Ley de Firma Electrónica Avanzada (in Spanish)
South America	• Privacy • Digital Signature • Cybersecurity	• Brazil's « Lei Geral de Proteção de Dados » (LGPD) and others • Colombia Law Nº 1928 of 2018 to prevent cybercrime

WORLD REGION	KEY POLICY ORIENTATIONS INCLUDE	REGULATIONS OR POLICY INSTRUMENTS (DECIDED OR PROPOSED)
Africa	• Privacy • Digital Signature • Cybersecurity • Data localisation	• 33 countries have data protection laws and/or regulations. • South Africa "Protection of Personal Information Act" (POPIA) • Kenya Information and Communication Act, Rev. 2009 • Ivory Coast Ley No. 2013-451 against cybercrime • In 2021, Rwanda, Zambia, Zimbabwe, enacted their first data protection law, Cape Verde, amended its existing legislation. Burkina Faso, replaced its 2004 Data Protection Act with a new one • In 2022, Uganda, Kenya, Senegal, and South Africa jurisdictions with a data protection legal framework also adopted and issued regulations and guidance • 2021 was also a year where stricter data localisation rules were introduced on the African continent
Asia	• Privacy • Digital Signature • Cybersecurity	• India Information Technology Act 2000 • Republic of Korea Digital Signature Act No. 5792/1999 (in English) • Korea Framework Act on Electronic Documents and Transactions (In Korean) • Republic of Korea Act on the protection of information and communication Infrastructure • Republic of Korea Act on Promotion of Information and Communications Network Utilisation and Information Protection • China 2004 Electronic Signatures Law of the People's Republic of China • Japan Unauthorised Computer Access Law, 2013 • Singapore Cybersecurity Act No.9/ 2018 (in English) • Thailand Cybersecurity Act B.E. 2562 (2019)
Oceania	• Privacy • Digital Signature • Cybersecurity	• Australia Electronic Transactions Act 1999, amended in 2011 • New Zealand 2015 The Harmful Digital Communications Act • Australia Online Safety Act 2021

2.3. Case Studies

USA:

Mobile Driver License in Florida

As part of its commitment to modernise its services, the Florida Department of Highway Safety and Motor Vehicles (FLHSMV) is launching its Florida Smart-ID, a secure and digitalised version of the driver's license on a smart device. The mobile driver's license is ISO 18013-5 compliant, when used with an associated Florida Smart-ID Verifier device, Florida drivers can provide safe, trusted, and contactless proof of identity, age, or entitlement to drive.

Target date of implementation
2022

Status
Deployment

Statistics
- 17.6 million potential users
- Smartphone penetration close to 100%

User benefits
- Protection against identity fraud
- Contact-free and convenient way to prove identity or age
- Peace of mind, identity credentials are always with the user, on his smartphone
- Offers advanced & value-added use cases (proof of age, identity attribute sharing, etc.)
- Enhanced user's privacy, citizens are in control of their data
- Secure access to online public services portals through strong mobile authentication

Other benefits
- Cost-efficient and fast to deploy for issuance authorities
- Easy to issue, update and revoke the digitalised credential
- Providing real-time accurate information
- Facilitate identity checks from anywhere (with or without connectivity)
- ISO 18013-5 compliant and usable in any other states/countries

Future Developments
- The application can be expanded as required to make every type of identity document available through the app

France:

New national identity card and digital identity program

To comply with new European regulations and provide the most secure identity document to its citizens, France has introduced a new electronic identity card that an anchor of trust for its digital identity program. The identity card is equipped with QR codes and a chip that contains the holder's digitised image and two fingerprint biometrics. In parallel, the French government agency, Agence Nationale des Titres Sécurisés (ANTS) has introduced its national digital identity program, France Identité Numérique. This enables French citizens to prove their identity remotely when completing online transactions by placing their new electronic identity card on the back of their smartphone and entering a PIN code to complete a high level of authentication.

Target date of implementation
2021

Status
Running

Statistics
- 70 million inhabitants
- 40 million users of the France Connect platform
- 900 service providers on the France Connect platform

User benefits
- Consent-based authentication
- Selective attribute sharing

Other benefits
- eIDAS high compliancy: Digital identity authentication via NFC leveraging the chip of the electronic identity
- Privacy by Design
- State-of-the-art biometric checks solution, NIST certified

Future Developments
- With the upcoming regulation on the EU wallet, this remote electronic identity card authentication can potentially be leveraged for the new French EU wallet

India:

Remote electronic signature using Aadhaar Digital identity

The Aadhaar program in India provides a digital identity base to build and deliver digital trust services that would be impractical without pre-existing digital identities. However, there are still challenges to ensure that the business gains of a pre-existing digital identity are not lost by inefficient design or integration of trust services. The remote electronic signature service is implemented by several registered CAs ensuring the preservation of digital identity value from identity creation to trusted identity use.

The cost of providing hardware tokens for digital identity in a market the size of India is prohibitive. The Aadhaar eKYC service can provide identity authentication and identity attribute information that may be used to register users and create signing certificates in real-time. This solution enables the use of the Aadhaar based digital identity for electronic signature services across different applications service domains. Originally designed to use the Aadhaar eKYC concept the same solution now also supports bank eKYC since 2020.

Target date of implementation

Several since 2018

Status

The solution is a major Aadhaar digital services use case, implemented by registered CA service providers to offer services to relying party application service providers in India. Today the eSIGN solution is deployed with several CAs in India and is fully compliant with the 2020 guidelines issued to CAs by the Controller of Certifying Authorities (CCA), Ministry of Electronics and Information Technology, Government of India

Statistics

- Aadhaar registers the full adult population of India to create a centralised digital identity

User benefits

- Support low friction user experience. The remote browser-based solution fits transparently within the hosting business web application
- No entry barriers. No need for a complex pre-registration process. Signatories use their existing Aadhaar, or bank issued digital identities to sign
- No new cost to signing users. No need for hardware tokens to support the use of signature keys
- Privacy friendly. Personal Identifying Information (PII) is stored only on the IDP side and not in the eSignature solution
- Services based on Aadhaar offline eKYC method limit central government visibility of digital identity use

Other benefits

- Electronic signatures have legal recognition in India since 2000
- Complies with CCA API, Aadhaar eKYC API, and India banking regulatory integration requirements
- The eSign system architecture obtains from the Aadhaar, or bank, eKYC services the necessary attributes to identity and authentication users without additional complex registration
- The authorisation of parties to sign is handled by the Application Service providers and the CA provider that hosts the eSign service
- Signing integration is based on the India Controller of Certifying Authorities (CCA) standard
- Easy API based integration to Aadhaar online eKYC and application service provider systems
- Use of Aadhaar offline eKYC based on CA download and PII identity data storage policies

Future Developments

- India's CA network likely to present more business to consumer (B2C) based signing integration solution support. CAs also likely to build more business on their use of the Aadhaar offline eKYC procedures.

Nigeria:

The challenge of farmers' inclusion in Africa

An insight into Digital Identity in Agriculture in Nigeria

Agriculture is one of the fastest-growing sectors in Africa. Today, there are about 33 million smallholder farms and the farmers that live on them contribute up to 70 percent of the food supply within Africa. Overall, the African continent contains 626 million people, and 384 million – or 61 percent – of them are farmers. In sub-Saharan Africa, economic growth from agriculture is 11 times more effective at reducing extreme poverty than any other sector. The Nigeria Bureau of statistics 2021 report states that the agriculture sector grew by 3.58% (year-on-year) in the fourth quarter of 2021, an increase of 2.36% from the preceding quarter, which recorded a growth rate of 1.22%. The sector contributed 26.84% to overall GDP in real terms in Q4 2021. There will be more than 9 billion people on the planet by 2050. That means two billion more mouths to feed by mid-century, this places more emphasis on the importance of sustainable agriculture through the introduction and implementation of global farming innovations. The current global food crisis is also an incentive to improve situation.

The challenge: According to the World Bank's ID4D statistics, nearly one billion people worldwide lack legally recognised identification. Another 3.4 billion people with one type of legally recognised identification face limitations in using it in the digital world. Smallholder farmers in Nigeria have complicated livelihoods because they typically rely on income from various sources, such as government safety nets, subsidies, and off-farm enterprises. According to a Creative Commons study, 78 percent of rural small-scale farmers in Nigeria suffer financial exclusion. Although slightly more than 27% were adequate in the access indicator – those with formal accounts – only 25% used legal or financial services regularly. Similarly, only one-third (31%) reported no barriers to economic participation, such as high transaction costs, lack of identification, and distance.

Using digital identity in Nigeria: Verifying and providing services to these farmers is primarily determined by data collection, which is prone to human execution error, unauthorised credential use, and the exclusion of individuals when done manually. Enabling these smallholder farmers to escape poverty will require creative solutions to critical challenges such as:

1 lack of access to financial services,

2 lack of adequate supply-chain traceability,

3 challenges related to the delivery of goods and services, and

4 gender inequality.

Many smallholder farmers struggle to access services and subsidies and seize new opportunities presented by innovations in mobile technologies, finance, and other fields, without official proof of identity. A robust and government-issued identity assist smallholder farmers in formally registering land and livestock and gaining access to mobile, financial, and other services that would allow them to work, sell, and spend income legally.

Outcomes: At least 13 federal agencies and several state agencies currently provide identity services in Nigeria. Each agency collects individuals' biometric information in the same way. Historically, the Nigerian government aimed to integrate digital identity systems as early as 2014, but progress has been slow. The initial roll-out of the card, also known as an 'eID,' was hampered by an inadequate partnership in the private sector. As of October 2019, only 19% of Nigerians had registered for the national digital identity. To reach more people, Nigeria's National Identity Management Commission (NIMC) collaborated with the World Bank in 2020 to develop an ecosystem model designed to increase coverage in which individual registers for a SIM card with a national identity.

The Nigerian government also aims to use the NIMC identity to provide a wide range of services, including financial inclusion, digital payments, employee pensions, agricultural benefits, and census. This form of digital identity (NIN tokens) makes it easier to promote flexible formal account opening and fewer restrictions on transaction operations, even for smallholder farmers. Additionally, there has been a demand for a biometric bank verification number to ease the challenge of financial inclusion. Both NIN and BVN give each farmer a unique, verifiable identity across formal institutions and, as such, reduce the problem of lack of identification. In the long run, digital identities will enable agricultural financing agencies and the government to verify farmers' identities quickly and promote increased access to financial services, efficient supply-chain traceability, and the eradication of gender inequality.

Mexico:

Improving the lives of pensioners

In Mexico, pensioners have to travel for hours, twice a year, in order to provide proof of life and thus be able to collect their pension. How could this required process be turned into something simpler for the pensioner but at the same time sufficiently secure against potential identity fraud for the bank?

Biometric technology has brought the solution: proof of life for pensioners; a transparent and secure process that allows verifying a person's identity through their voice, with a single call from any device, at any time, in any place, in any language or dialect, and with just 3 seconds of their voice.

Implementing this system is a step further in favour of the financial inclusion of the elderly and other ethnic groups with different language backgrounds, enhancing the prevention of potential fraud and achieving enormous cost savings.

This solution has already been implemented in BBVA Mexico, one of the leading European banks in asset volume, number two in Spain, and Mexico's largest financial institution. What has allowed that, for the first time in the industry, senior citizens could provide proof of life in Mexico without needing to go physically to bank offices. Instead, a 3-second phone call is enough to collect their monthly pension allowance. To date, more than 105,000 pensioners have registered with a success rate of +99.9%, and more than 165,000 pensioners authenticated with a success rate of +95%.

3.
Section 3.

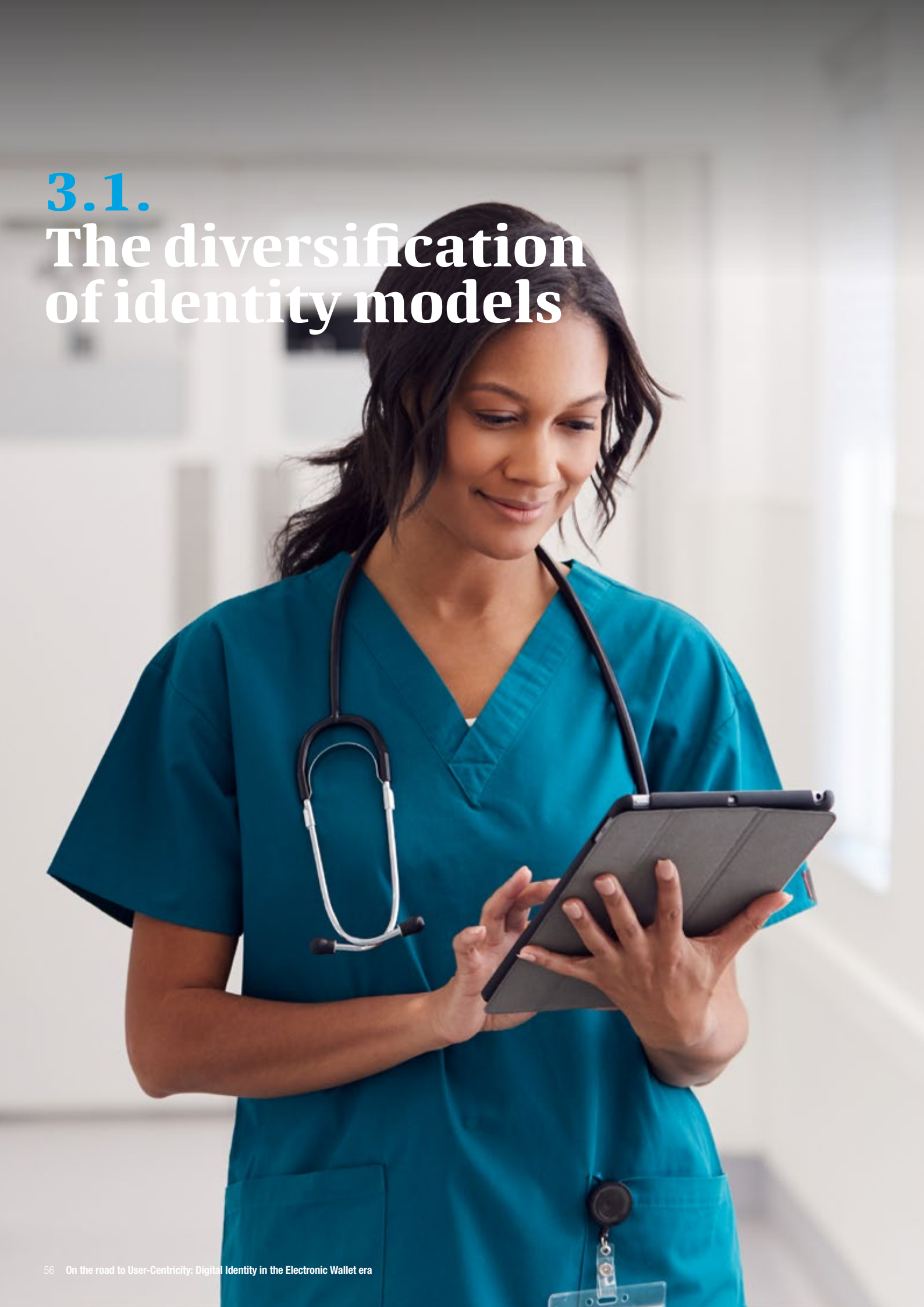
Introduction

Since 2020, the global shift to the digital paradigm for services has created an opportunity for the further diversification of digital identity models. It has also resulted in new stronger interoperability standards and the emergence of new technologies.

In this final Section we evaluate in detail the advantages and drawbacks of centralised, federated and de-centralised data models, and explore some key digital identity standards that are evolving. After which we look at some promising technology developments on the horizon and examine how interoperability will be key for success.

Governments are becoming increasingly responsible for assuring the proper governance of their national identity digital ecosystems. This entails structuring appropriate trust anchors, considering the legal liability landscape, and adopting international standards for greater interoperability.

3.1. The diversification of identity models



When talking about identity models, there are several criteria that need to be considered. These include:

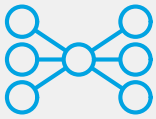
- Who is the main data controller and/or identity issuer and/or trust anchor in the ecosystem?
- What is the level of stakeholders' engagement: public services, private sector, and natural persons?
- How are flows organised between users, service providers, and identity or credential issuers?

Functional digital identity is underpinned by three key architecture models: centralised, federated and decentralised. Typically, all three models co-exist, due to their respective advantages. Proving that 'no one size fits all' in functional digital identity domains.

Main Identity conceptual models

Centralised

- Central authority considered as the main identity provider and the data controller
- For functional digital identity, a variant is that the service provider is also the identity provider
- Hierarchical trust framework or ecosystem
- E.g. Canada, Denmark, Estonia, India, Nigeria, Singapore



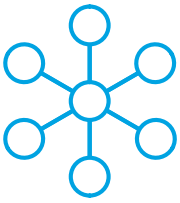
Federated

- There are several identity providers public and private, and many service providers
- Users have the choice to use various credentials
- Federated trust framework or ecosystem
- E.g. Bank ID scheme in the European Nordics countries (Sweden, Norway, Finland, and Denmark) In Southern Europe, France Connect or SPID in Italy

Decentralised

- Users are considered their own data controller – They select attributes and authorise parties to verify credentials
- Technology systems remain as the main/only "intermediation layer" with decentralised architecture and registries
- The "self-sovereign identity" concept is a candidate for this model
- E.g. Switzerland is developing a decentralised architecture identity layer over centralised or federated solutions at cantonal levels. Canada, Estonia, Spain, and the US are developing various proofs of concepts and models

3.1.1
The centralised model



Centralised models characterise an entity as being the main authority and data controller. In foundational identity, the national state acts as the root of trust through official registries and identity credentials. When we talk about functional digital identity, we often mean that the service provider is also the identity provider. When talking about a digital ecosystem, we sometimes talk of the centralised model in the way that data repositories are controlled by public authorities or that there are only a limited of identity credential issuers, usually from the public sector.

In terms of how it works, there are usually one or two reference public identity providers that can be used for public digital services and sometimes private services too. The alternative is to use an account for each service provider that also performs the role of the identity provider. Sometimes the centralised service is mandatory for enrolment before using federated or decentralised authentication. Sometimes the service delivers the full cycle of enrolment needs: onboarding, passwordless authentication, a data platform for attribute attestation and authorisations, and signature services.

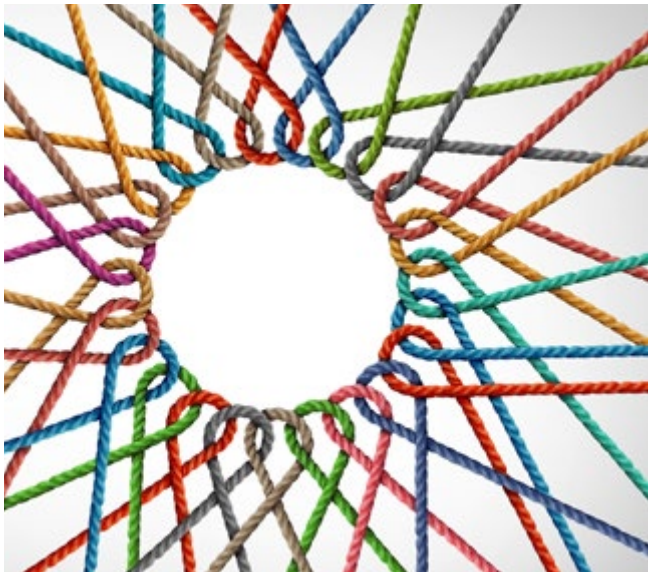
Advantages - achieving a degree of state data sovereignty and the synergies of just one or two specialised entities delivering functional digital identity services to businesses and citizens. The model is most appropriate for small-sized countries (less than 8 million inhabitants). Estonia and Singapore are fine examples of good centralised model implementations. However, Aadhaar in India or NIMC in Nigeria show how large countries can also successfully implement a centralised model.

Drawbacks - potential drawbacks are linked to a potential single point of failure, data capture or privacy risks, and to the inability of the state to assure the cumulative roles of the identity provider, the data controller, and the identity governance rule maker and management. When the centralised model refers to a single company assuring both services and identity provider role, the potential risk is of lesser ergonomic due to lack of specialisation and poor account management with a risk of users going away from the digitally provided services.

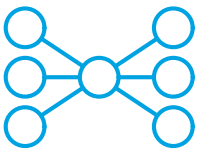
How to get it right - it is advisable to have a well-defined governance system, including certain independence for the identity authority, strict roles management between sub-agents or sub-entities, separation of duties, internal and external audits on policies and processes together with an independent entity for privacy risks and practices monitoring. When a service provider is also an identity provider, it needs to evaluate the gains and losses of evolving toward a federated model or a decentralised one. There are critical factors to becoming its own identity provider regarding size, number of users, and user activity. If you do not meet the required criteria, you may use alternative identity providers under this model (public identity providers) or under the federated model.

Outlook/perspectives - while centralised models will continue to exist/develop in many parts of the world, more and more hybrid models are emerging where centralised models (for instance in the public sector) interface with federated models (in the private sector/on the Internet) and sometimes with decentralised models. Switzerland and Canada are examples of two countries where all three models coexist at different levels: national, federal, local, or specific.

Example countries - Canada, Denmark, Estonia, India, Nigeria, Singapore



3.1.2
The federated model



The federated model allows individuals to use the same digital identity credentials to access various online services or use a variety of public or private identity provider's credentials to access one service. This mix of centralised and federated model overcomes the disadvantage of having to create multiple accounts throughout the network while usually offering a variety of private or public identity providers to the users.

In terms of how it works, thanks to specialised private and public identity providers, identity data and user accounts are managed by third-party solutions. Modern solutions will give users a passwordless experience that avoids the need for multiple user credentials and passwords for several online services. Plus, users, and businesses can completely rely on external service providers.

Advantages – federated identity gives better service access/ergonomics to users, allowing users to use the same credentials to access multiple online services in a secure/convenient way. Built on tried and tested protocols and schemes, when implemented correctly by actors such as governments or banks, users have full control of their data and how it is shared with relying parties. Given its technical maturity, integration into the ecosystem is fast and easy using standard and freely available solutions. Today, all government identity schemes rely on federated identity in some shape or form.

Drawbacks – federated systems do not guarantee a high level of privacy and are dependent on correct and transparent implementation. Some public identity providers will try to serve as many sites as possible and will therefore adopt relatively low-level privacy and security notices, with little protection of the user's digital identity data (the risk of having Internet giants abusing our data and overlinking online behaviour with social logins exists). Also, a data leak at the identity provider level could lead to unauthorised connections to many services. These security and privacy issues mean that only reputable identity providers should be trusted with sensitive digital identity attributes, such as a digital passport or financial data.

How to get it right - three generations of federated identity protocols have been developed since 2005 - SAML (Security Assertion Markup Language), OAuth, and OpenID Connect. Thanks to these protocols, single sign-on (SSO) is now a standard feature of most enterprise intranets and extranets.

Start by mapping out your technical requirements for seamless integration with your information systems and make sure to assess your team's capabilities to lead the integration, without sacrificing compliance, user-friendliness, or technical flexibility. Depending on your requirements, choose the identity provider that can cater to your needs.

Outlook/perspectives - with the massive adoption of federated identity solutions, most protocols used are becoming de-facto standards and federated identity continues to contribute to interoperability in identity ecosystems. There has been much effort to raise the levels of enrolment, credentialising, and authentication processes using both static and dynamic trust management techniques. Many initiatives including passwordless and secure Sign-In are coming live to continue to improve convenience, privacy, and security. The adoption of new protocols to secure the online authentication processes are also increasing. In 2022, some tech giants announced common initiatives to adopt passwordless sign-in for all their products and services using online protocols as those developed by the FIDO Alliance and the W3C.

Example countries - The Bank ID scheme in the European Nordics countries (Sweden, Norway, Finland, and Denmark) is a good example of a federated identity scheme. In Southern Europe, France Connect or SPID in Italy are both examples of successful hybrid centralised-federated identity schemes with over 30 million users in each country in May 2022. In the US and in Australia several private identity providers interact within federated identity models to access public and private services. On the web, OpenID Connect has made it possible for the public to use the login buttons of major technology companies, on many Internet Social Networks.

3.1.3
The decentralised model

Decentralised identity can be defined as a mechanism that allows users to directly manage their digital identity using a distributed architecture. This architecture can use decentralised ledger technology (DLT) or another trust layer together with digital identity wallets. Instead of manually creating and managing accounts (centralised identity) or trusting identity providers (federated identity), decentralised identity places the individual at the centre of each of its digital interactions. To this end, decentralised identity is based on a peer-to-peer relationship between three parties:

1. **The issuer** - in both physical and digital life, each credential is generated by an issuer. The issuer is the source of the credentials that prove a person's identity attributes - the author of those documents, so to speak. Most issuers are entities such as government agencies (e.g., Department of Motor Vehicles for driver's licenses) but they can also be financial institutions (bank statements), energy providers (utility bills to prove home address), and so on.

2. **The holder** - the person who wishes to prove his or her identity or log on to an online service. The identity holder requests proof of identity from the issuer in the form of a verifiable credential. The identity holder then stores these credentials in their digital wallet for presentation to verifiers when requested. At the centre of this tripartite relationship, the holder always has the choice of whether to reveal their identity attributes. It should be noted here that in certain use cases, such as for the management of the identity of a legal entity in civil law jurisdiction, a distinction can be made between the holder and the identity subject. Indeed, if the holder is generally the same person as the identity subject in some cases, it may also be a third party that stores the identification information on behalf of the identity subject.

3. **The verifier** - any person or entity that wants to verify the digital identity of an identity holder to allow him/her to exercise his/her rights or to use a service. For example, an insurance company wants to verify the address of its customer to provide them with homeowner insurance. If the identity holder agrees to reveal his/her information, the verifier will check both the presented digital identity as well as its source. In particular, the verifier ensures that the issuer's digital signature is present in the certificate provided. This last verification guarantees digital trust and considerably reduces the risk of fraud.

In some ways the tripartite model of decentralised identity replicates what we experience in the physical world. In everyday life, if an individual wants to prove his address, for example, to join a gym, he/she will show his/her identity card to the person in charge of his/her registration. This proof of identity will be authentic because it is itself issued by a trusted third party. With decentralised digital identity, it's the same thing: the individual will simply be able to prove his/her digital identity through the credentials stored in his/her digital wallet. The verifier will then be able to ensure that this certificate is not fake since it is signed by its official issuer.

Advantages - with the rise of distributed ledgers and blockchains, the prospect of experiencing more privacy control of the data exchanged through the Internet is rising. Some countries as in Canada, are experimenting and building provincial platforms using SSI and Verifiable Credentials to deliver cloud and mobile based digital identity services to their citizens. These services are looking also at future interoperability based on W3C built standards to develop decentralised solutions for authentication and verification purposes. Decentralised identity solutions bring key advantages to final users such as control over their data, respect for their privacy, and compliance with regulations in place.

Drawbacks - at this stage as the technology is still maturing, challenges remain for users, the ecosystem itself, and on the general environment. Putting more responsibility on users using sophisticated technology layers can be a challenge. The user's challenge exists on appropriate use of the technology, on individual behaviours related to security and finally legal challenges regarding user responsibility as potential data controller and identity issuer/ manager. The ecosystem challenges tend to be related to the economic viability of finding an appropriate business model and to the new and still incomprehensive standards layer (although these are evolving fast) that can hamper effective interoperability between systems and platforms and raise security concerns. The governance frameworks should be also strengthened in time. Finally environmental challenges do exist as, for instance the need for human assistance, regulatory constraints (e.g., financial sector with anti-money laundering business practice), and energetic expenses of some blockchain based solutions.

3.1.3
The decentralised model
(continued)

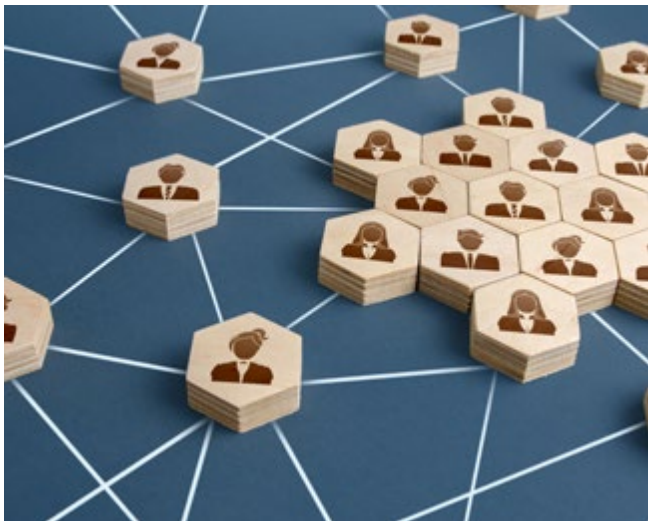
How to get it right – a variety of implementation approaches are currently being evaluated. For instance, proof of concept and pilot use cases with growing perimeters and experimenting with various public or private ledger registries. Governments can ill afford to completely replace what works today for the 'promise' of decentralised identity. In the private sector, successes in finance and banking also need improvement, with a high level of identity assurance. Meanwhile, decentralised identity is gaining traction with many standards bodies including the Decentralized Identity Foundation (DIF) and the World Wide Web Consortium (W3C).

Outlook/perspectives - several governments are experimenting with decentralised identity architectures and use cases look set to grow following progress on standards implementations and interoperability.

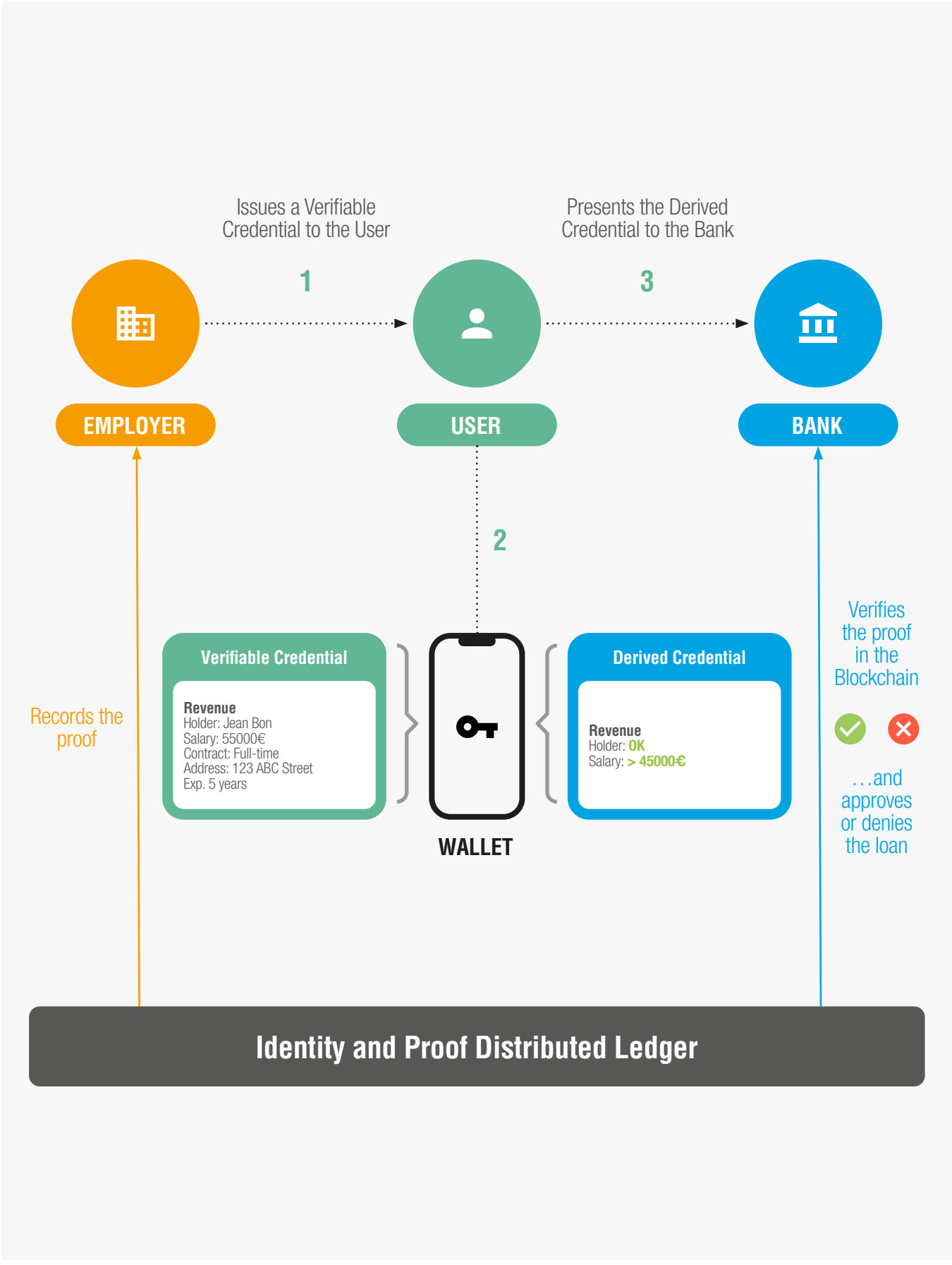
With the tech sector eager to invest in this emerging market, big tech companies have already registered patent claims related to 'verified claims of identity' and are pursuing decentralised options in a similar way to how their proprietary wallets already control the presentation and verification of traditional forms of identity like driver's licenses and passports [REF16].

There is growing potential in the broad adoption of W3C Verified Credentials to facilitate the acceleration of digital identity trust and interoperability under the Decentralised Identity Architecture model.

Example countries: Switzerland is developing a decentralised architecture identity layer over centralised or federated solutions at a canton level. Canada, Estonia, Spain and the US are developing various proof of concepts and models.



Asking for a loan using verifiable and derived credentials



3.2. The evolution of standards and technologies

3.2.1
Assessment is a top focus for standard and technology governance

Technology governance largely takes the form of technical standards and groups of competent third parties that assess if these standards are correctly implemented. Some of these standards are specific to the implementation of identity concepts, such as the implementation of secure electronic signature creation devices, or more recently with standards such as W3C for decentralised identities, but there are also standards that address the technology used to present services. For example, standards such as ISO 27001 consider the risks faced by technical informatics-based services, providing best practices on how such risks should be managed. The wide scope of technical standards, many of which are new, brings new governance challenges and all too often the dream exceeds the reality, in terms of what can be designed, built, and governed safely.

A single governance model for all relevant standards in digital identity is unlikely to prevail, but there is a generally accepted principle that for high-risk or high-security assurance solutions, the independent validation of design and operations should be included.

Despite the desire of nation-states to own the governance of national digital identity technologies, many government administrations lack the in-house competence required to validate complex security architectures/technologies. As a result, they delegate this responsibility to a 'qualified' third party; an arrangement that has become formalised in Europe.

As well as having a designed body (or agency) responsible for the supervision of digital identity and the policies associated with this, national governments should also build a technical governance level that ensures the responsibility of assessing and auditing the various technology solutions is passed to one or several Conformity Assessment Bodies. These bodies act as a link between the technical and the decision policy level. As digital technologies refresh and diversify then conformity assessment becomes more complex and a new part of the digital identity value chain.

In the era of digital wallets, standards are becoming increasingly important for functional digital identity and continue to play a key role in the technology maturing process and adoption curve. They are also increasingly required to achieve interoperability, and to ensure trust is applied to architecture models and emerging ecosystems worldwide.

3.2.2
Three evolving digital identity standards

We believe the following three standards will prove highly significant in the digital identity arena. Following a short overview, we describe some of their potential for the future.

ISO 18013

3.2.2.1 ISO 18013-5

In September 2021 ISO published the fifth part of a series of standards on private information on drivers licenses - the ISO/IEC 18013-5 Personal Identification – ISO-Compliant Driving Licence – Part 5: Mobile Driving Licence Application with the goals of interoperability, extensibility, security, and privacy.

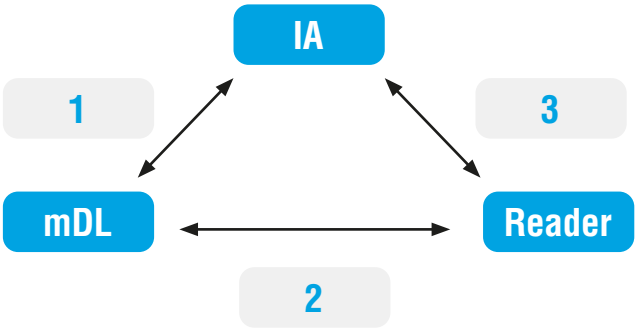
At a glance....

- Primary focus: implementation of a driving license in association with a mobile device.
- Potential evolution: model for implementing identity credentials or derived official documents in association with a mobile device.
- Technical perimeter: interface between the mDL holder and the mDL reader and the interface between the mDL reader and the issuing authority infrastructure.

Introducing the standard in more detail

A mobile driving license (mDL) is a mobile app that holds a digital representation of a physical driver's license. It aims to make customer interactions more efficient and accurate and enable new use cases by preserving security and privacy. In that sense, a mDL is not just a picture of a driver's license stored on the user's smartphone as this is not trustworthy at all. ISO 18013-5 provides mechanisms to obtain and trust the data from a mDL.

The basic simplified architecture



- **Interface 1** describes the interaction for mDL provisioning, data-signing, issuing, and life cycle management. This is typically done by the issuing authority. This interface is out of the scope of ISO/IEC 18013-5 but will be part of the upcoming ISO/IEC 23220 series of standards
- **Interface 2** (fully specified in ISO/IEC 18013-5) describes the interaction between an mDL holder and the mDL reader (short-range) to establish a secure connection, perform authentication and share attributes. Data is exchanged using NFC, BLE or Wi-Fi-Aware.
- **Interface 3** (fully specified in ISO/IEC 18013-5) describes the remote interface between mDL reader and mDL issuing authority to allow for server retrieval of data. This interface is optional for the mDL reader and issuing authority.

The current version of the standard covers in-person use-cases only where the holder and verifier are interacting next to each other. Identity verification is performed against the portrait picture of the holder which is obtained from the mDL. The interaction of a holder with a remote verifier is currently being investigated in the next version of the standard.

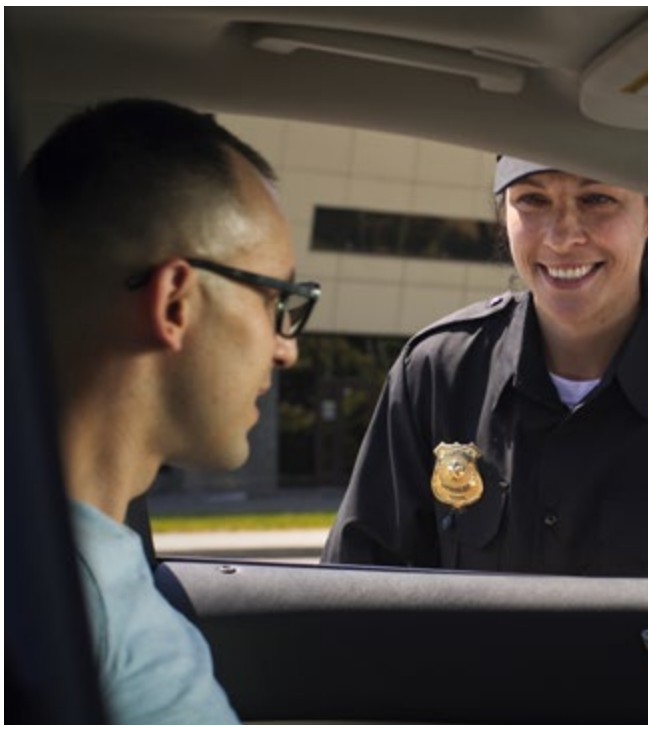
The information exchange process

The process of verification is initiated by the mDL holder who engages with a verifier over a QR code or NFC. The exchanged information (called Device Engagement) contains all details necessary to set up a secure connection between mDL holder and reader. The Reader only asks for the data needed and the two devices can then exchange the signed data over BLE, NFC or Wifi-Aware. In attended use cases the portrait image should always be requested. The reader can verify the signed data by checking the signature of each individual data element. The standard makes use of well-known security mechanisms such as passive authentication (ensures that data is genuine and unchanged) as well as active authentication (ensures that data was not cloned from a different device). During data transmission, the portrait image is transferred and displayed on to the Reader the verifying person can confirm that the mDL Holder is the person standing in front of him. User consent is not standardised. Nevertheless, handing over the Device Engagement code means consent has been given to connect to the mDL reader. In addition, consent for data transfer should not be granted by the mDL holder unless they are satisfied with the purpose of sharing specific data and know the mDL verifier with whom they are sharing.

Besides exchanging information between devices it is also possible for the mDL reader to obtain driver's license data from the issuing authority, directly over the internet using OpenID Connect or a Web API. For the mDL reader to retrieve information directly from the issuing authority, the Device engagement information should be enriched with an Identity Token hint.

Potential enhancements

Within the development of ISO/IEC 18013-5 expendability was of high importance.
The described data model provides sufficient flexibility for other digital credentials besides the mobile drivers' licenses. This can be achieved by defining a new document typo or a new namespace for specific data elements of the new document/credential.



3.2.2
Three evolving digital identity standards (continued)

ICAO DTC

3.2.2.1 ICAO DTC

Another important evolving standard in relation to digital identity and wallets is the ICAO initiatives on Digital Travel Credentials [REF17] and Visible Digital Seals that can also be used for health certificates, emergency travel documents, or Visa attestations [REF18].

In October 2020 the ICAO published version 4.4 of its *Guiding Core Principles for the Development of Digital Travel Credential (DTC)*. Passport dematerialisation has become a top priority following COVID-19 and DTCs and Visible Digital Seals (VDS) are considered by ICAO as fundamental supports for digital identity and attribute assertions.

At a glance...

- Primary focus: making travel more efficient. The DTC verifiable credentials can be provided in advance by the traveller to establish Advanced Passenger Information (API) and Passenger Name Records (PNR) and establish airport seamless flow.
- Potential evolution: attribute exchanges for airport or travel services; linking with Digital Visible Seal to provide rights attribute attestation.

Introducing the standard in more detail:

Technically, the DTC consists of two parts:

- A **virtual component** that represents the data. Containing the structured data of the identity conforming to LDS (Logicial Data Structure), this file can be stored on any medium whose security is based on a cryptographic link with the physical component (physical component). The DTC file stores both biographic and biometric passport data, in addition to bearing digital signatures which makes it verifiable.
- A **physical component** with cryptography and communication capabilities such as an electronic passport, a smartphone, or a connected watch. This is carried by the traveller as proof of possession to increase the passenger's level of identification.

The main features of the ICAO DTC are as follows:

- DTCs can be created as derivatives of electronic passports (extracting the data in the chip); and/or issued in parallel to, or as a substitute or replacement of physical electronic passports.
- DTCs contain, in a mobile and globally interoperable container, the holder's facial image, personal information attributes, and the requisite security features to support authentication.
- All generations of the DTC are backward compatible.

The DTC issuance process

The standard's documentation describes three variants for DTCs issuance:

- **DTC issued as eMRTD Bound:** The Digital Travel Credential is generated by the user in its own smartphone or from a self-service kiosk by reading the chip in their passport. The passport is considered the physical component.
- **DTC issued as eMRTD-Physical and potentially bound to another device:** The Digital Travel Credential is issued and digitally signed by a passport issuing authority. In addition to being linked to the passport, the DTC may be linked, by cryptographic mechanisms, to an additional "physical component".
- **DTC bound to independent Physical component:** The Digital Travel Credential is issued and digitally signed by an issuing authority independently of a passport and linked with a hardware device (mobile phone or other connected device). The DTC has its own lifecycle.

Potential enhancements

Enhancements include better integration with governments systems to increase the free flow and security of travel. For instance, with the European Union, integration with EES (Entry/Exit System) and ETIAS (European Travel Information and Authorisation System). It is also allowed to envision further attributes exchanges (health, travel services, customs) authorised by the holders.

3.2.2
Three evolving digital identity standards (continued)

W3C - VC

3.2.2.3 W3C - VC Credentials

As digital identity becomes central to life worldwide, public concern has been growing about businesses built on the monetisation of personal identity information and increasingly proprietary platforms are being viewed as creating de facto risks for users' privacy and trust.

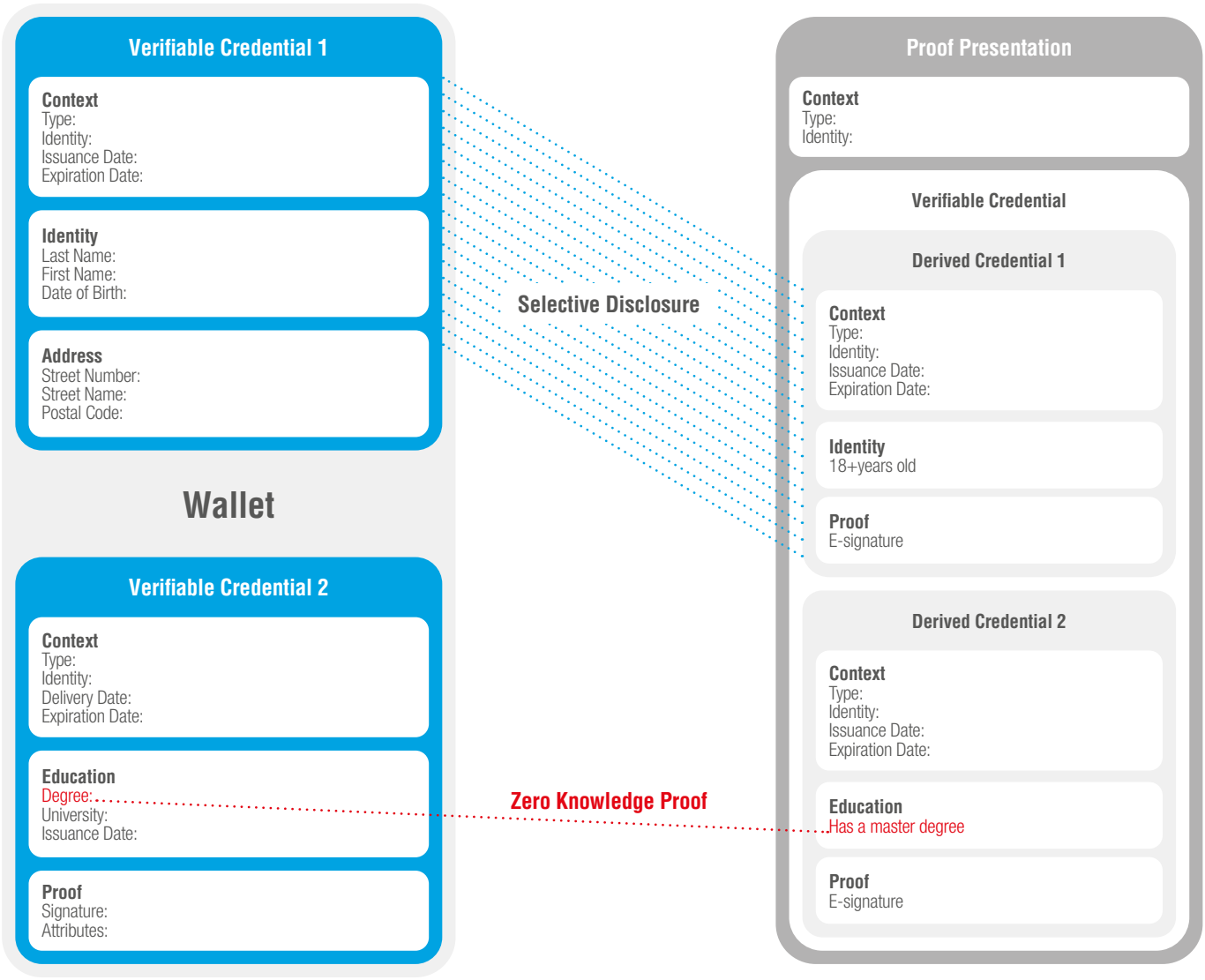
With the rise of blockchain and distributed ledgers, the prospect of experiencing a decentralised, self-sovereign, and privacy-friendly Internet is progressing. Enshrined in this Web3 philosophy and a Self-Sovereign Identity approach, since 2017 W3C has been building standards to help actors develop decentralised solutions for authentication and verification purposes: Decentralised Identifiers (DIDs) [REF19] and Verifiable Credentials (VCs) [REF20].

At a glance....

- Primary focus: provide a data model that can be protected by a variety of current and future digital proofs.
- Potential evolution: interoperable attribute exchanges in a decentralised environment.
- Technical perimeter: W3C-VC goes further than a cryptographically signed attribute as it is most often used together with Decentralised Identifiers another W3C standard. Their association is emphasised as one of the preferred ways to implement the concept of Self-Sovereign Identity.

Introducing the standard in more detail:

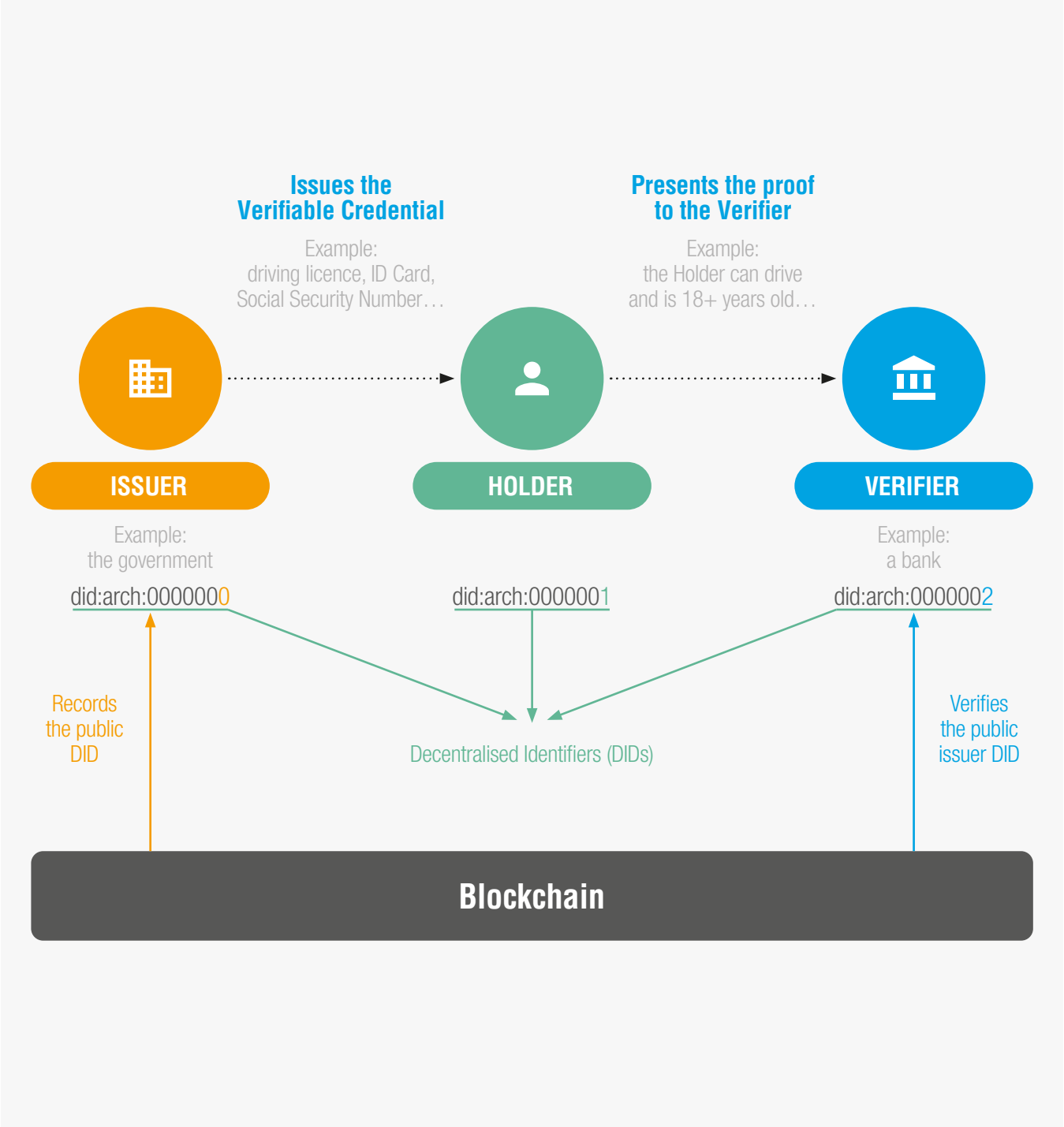
- **Self-Sovereign Identity (SSI)**
  SSI is an approach where the individual can control and manage his/her own digital identity, without the intervention of a centralised trusted party. This user-centric approach is currently missing from most user experiences on the internet, where digital identities are stored and managed by online service providers.
- **Decentralised Identifiers (DIDs)**
  A DID is a unique identifier that refers to a subject like a person or an organisation. As opposed to federated identifiers attributed by a third party, DIDs are decoupled from centralised registries and are related to a specific distributed ledger. The way it's built allows DID controller to prove control over it without requesting permission from any other party. It's designed to facilitate authentication to specific services online.
- **Verifiable Credentials (VCs)**
  A VC is a standardised digital certificate issued by an authority that certifies specific attributes tied to an entity. VCs can refer to information such as names, identification numbers, passports or driving licenses. It's cryptographically secure and respects the privacy of the user. A VC is bound to a DID which is therefore linked to an identity. Decentralised identifiers, verifiable credentials, and self-sovereign identity represent the face of Web3 allowing every user to read, write his/her own pieces of the internet in a privacy-friendly manner. By introducing these standards to the web community, the W3C is advocating for a new Web for all.


Verifiable Credential 1
Context
Type:
Identity:
Issuance Date:
Expiration Date:
Identity
Last Name:
First Name:
Date of Birth:
Address
Street Number:
Street Name:
Postal Code:
Wallet
Verifiable Credential 2
Context
Type:
Identity:
Delivery Date:
Expiration Date:
Education
Degree:
University:
Issuance Date:
Proof
Signature:
Attributes:
Selective Disclosure
Zero Knowledge Proof
Proof Presentation
Context
Type:
Identity:
Verifiable Credential
Derived Credential 1
Context
Type:
Identity:
Issuance Date:
Expiration Date:
Identity
18+years old
Proof
E-signature
Derived Credential 2
Context
Type:
Identity:
Issuance Date:
Expiration Date:
Education
Has a master degree
Proof
E-signature

3.2.2
Three evolving digital identity standards (continued)

Potential enhancements

The large scope and openness of Verified Credentials in the W3C standard looks promising for many usages related to the Web and to the digital wallets. However further work is required to be able to support the security and reliability of proof models, data transmission protocols, and interoperability implementations for sensitive risk or trust use cases.



3.2.3
New digital identity standards

New standards are arriving in the sphere of digital identity. As we have seen with ISO 18013, ICAO DTC, and W3C-VC, these standards are often linked with the development of digital wallets on mobile phones for presenting credentials and/or attested attributes or data.

Stakeholders should select standards carefully to ensure they are able to:

- Achieve the best possible relationship between standards/architecture models.
- Make sure the chosen standards are mature enough including in data storage, attribute transmission, and effective implementation.
- Achieve interoperability with other digital identity standards used in the ecosystem - ISO23220 (credential issuance and sharing), Open ID Connect (for online authentication), or OSIA (Open Standards Identity APIs) for interoperability of foundational identity management systems [REF21].

Data standards: a comparison

To create a world in which cooperation-competition is able to thrive, future standards for digital identity look set to become converging rather than competing. Currently, there are several large-scale pilot projects underway where the use of several standards in supplementary modes is being considered.

	ISO 18013-5	W3C/VCS	ICAO DTC
Data transfer	Several protocols defined (NFC, BLE, WIFI Aware, internet	Different implementations are being worked on	BLE, NFC
Data model	Very flexible data model that covers data representation, transmission technologies, data element definitions	Focuses on the data model and doesn't cover mandate data representation syntax, transmission technologies, data element definitions	ASN.1 based on travel documents
Data storage	Stored either on the holder's mobile device or on a server from the issuing authority	Holders must be able to store Verifiable Credentials in any location	Virtual component (VC) and physical Component (PC)

3.3.
Case Studies

Singapore:

"Singpass" digital identity

"Singpass" is an abbreviation for "Singapore Personal Access" and represents the flagship of Singapore's digital transformation. It is mainly a gateway for government services and other e-services and includes a mobile application with the same name (Singpass app). Singpass is now a multi-functional digital identity product including many features for identification and enrolment, authentication (including password less and multibiometric), authorisation (incl. digital signature), and exchanging or sharing attributes with consent.

The main orientations for Singpass are to improve the lives of the citizens, create business opportunities, and transform and extend the capabilities of government agencies.

Target date of implementation

First version in 2003, Last version in 2022 including business services

Status

Running

Statistics

- 4.5 million user-base (97% of Singapore residents aged over 15)
- Over 3.5 million users for Singpass App
- Over 2000 services from 700 service providers
- Transaction volume around 350 million per year

User benefits

- Large multifunctional digital Identity
- Derived digital Identity can be presented through the mobile app
- Inclusion oriented (e.g., MFA can be made through trusted family phones)
- Accessibility features (disabled people, cognitive or emotional deficient people)
- Corporate version (Corppass) with access to 130 government services and business roles for owners and managers

Other benefits

- SSO and prefilling data forms of digital data request (save time)
- Trusted onboardings with better data quality for service-providers
- Can be used for physical access to corporate or agency premises
- Digital signing through always at hand through the app
- Mobile document wallet with sanitary credentials (Covid-19)

Future Developments

- New services and mobile document wallet credentials

Source "Smart Nation Singapore"

Bank ID in the Nordics

The Nordics have become successful with digital identity using an original approach of a federated identity model based on bank cooperation to establish a scheme and then a successful ecosystem. While there are differences in all four countries (Sweden, Norway, Finland and Denmark), each ecosystem features banks that typically do the onboarding. In the early 2000s, the banks decided not to compete on identity or security and managed to cooperate to set up a common scheme. The digital identities were soon accepted by other players, including the respective governments.

Country or Region:
Norway, Sweden, Finland, and Denmark representing around 26 million inhabitants. Today more than 95% of the population of these countries use their digital identity on a regular basis. Please note that "BankID" is not an accurate term for all countries. In Norway and Sweden, the most common digital identity is called BankID, although the BankID of Norway and BankID of Sweden are separate, they only share the name. Denmark has just transitioned from NemID to MitID, and in Finland there is FTN - Finnish Trust Network.

Target date of implementation
Between 2003 -2010 depending on the countries involved

Status
Running

Statistics
- 90% of transactions or services accessed are within the private sector
- On average active user make 4-10 transactions per week
- Mobile bank identity launched between 2012 and 2020 have taken undisputed leadership in the preferred support to use digital identity

User benefits
- Bank-issued identities are today used for a lot of different purposes, from applying for a mortgage and university to registering the name of your children at birth or accessing multiple services while asserting rights and duties
- The health portal, where you will see appointments, vaccines, and other health info
- Digital Signing: If you buy and sell electricity, you may sign up with BankID. Student housing contracts are typically signed with BankID
- Attribute attestation of age

Other benefits
- Economy, efficiency, and productivity for public services
- Developing usages for business
- True federation – Example Norway while BankID is the most common electronic identity in this country, there are others as MinID (government issued), Buypass (required if you want to gamble) and Comfides (mainly used by health personnel). All of these can be used for government login

Future Developments
- Mobile wallet convergence (identity/payment)
- Evolution toward Cashless Society
- European and International Interoperability

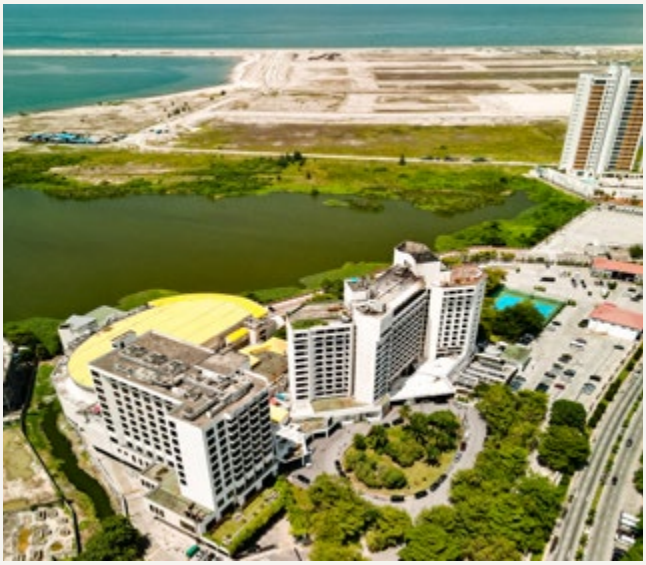
Nigeria:

Tokenization of Unique Numbers

The National Identity Management Commission (NIMC) is fostering privacy by developing the use of tokenized versions of the National Identity Number (unique identifier). The virtual NIN expires 72 hours after being generated.

The NIN tokenization solution was introduced as part of the Federal Republic of Nigeria's commitment to safeguard against identity theft and comply with global best practices, as well as preventing the blatant misuse, collection of personal data without required user consent, storage in an unencrypted and insecure database and misuse or negligent Processing of the NIN by data processors and third parties. This feature of the NIN Verification Service (NVS) is designed to provide enhanced privacy protection for the personal information of individuals registered in the National Identity Database (NIDB) and issued a NIN. Also known as a virtual NIN, the version is a tokenized version of the person's real NIN that cannot be stored or used by the verifying party in a way that compromises the confidentiality of the person's data.

The general goal of tokenization is to provide a codified representation of the real NIN for which another party verifying the identity of the registered person cannot maintain and use in a way that puts the individual's data privacy at risk.



Target date of implementation
2022

Status
Deployed and running

Statistics
- Over 71 million user-base and counting
- Digital penetration of NIN and Sim linkage
- 49 special enrolment services in Nigeria
- 19 Diaspora enrolment services

User benefits
- Provision of data privacy and protection of personally identifiable information
- Protection of the sensitivity of the NIN issued by the NIMC to registered individuals
- Provision of a visual, high-security representation of the National electronic identity on IOS and Android smartphones
- Promotion of a secure means of presenting NIN in a format that can protect the NIN from seeding, cloning, and duplication
- Tokens can be presented through the mobile app and expire after 72 hours

Other benefits
- More convenient onboarding with better data quality for service providers
- Seamless Data privacy protection for customers- access to an individual's NIN by others is further restricted
- Virtual NIN tokens generated are merchant-specific, a token generated for a company cannot be used or verified by another company

Future Developments
- The application can be extended as needed to tokenize other types of identifiers through the app

Colombia:

Mobile identity wallet Cédula Digital

The National Digital transformation plan has been materialised with a combined issuance of a new identity document and a Mobile identity wallet named Cédula Digital. The new Colombian Cédula Digital securely grants citizens access to remote services and allows in-person identity verification based on the latest industry standards.

The Cédula Digital is generated automatically from the moment the new identity card is issued. Once citizens withdraw their Identity card in an official physical branch and perform the first biometric checks, they receive a QR code and a unique activation link by email. They can use either of them to activate their Cédula Digital. They just need to download the national Cédula Digital application available on their mobile's Operating Systems respective App Stores and scan the QR code or click on this link to launch the digital Identity onboarding process. The onboarding process requires the following steps:

Face verification: the citizen is authenticated using the latest facial recognition technologies – a selfie is automatically compared to the photo recorded in the national civil identity register.

PIN creation: the citizen creates a 6-digit security PIN code, and the Cédula Digital is ready to be used.

With the Colombian Cédula Digital, identity attributes are securely stored in the citizen's device. Citizens can select attributes they consent to share according to the usage, which protects their privacy. Citizens can also display a full digital rendering of their identity card directly on their smartphone.

Online: citizens can authenticate themselves remotely via a simple selfie and access online services.

In-person: through a dedicated verification application, for instance, a police officer can automatically verify identity attributes after a person has given consent.

Target date of implementation
2020

Status
Running

Statistics
- 51 million inhabitants
- 3rd place in the OECD's ranking on the digitalisation of public services
- 79%* of unique mobile subscribers, including 67% of smartphone adopters

User benefits
- Multifunctional wallet solution
- Consent-based authentication
- Selective attribute sharing

Other benefits
- Scalable approach with the wallet opportunity
- Privacy by Design
- State-of-the-art biometric checks solution, NIST certified

Future Developments
- The app can be expanded as required to derive other official documents and make them available in a secure way on the mobile phone

Digital identity in the Metaverse

After Facebook's name changed to Meta, the Metaverse has made news around the world. International brands such as McDonald's and even countries like Barbados are opening digital offices and implementing projects in this virtual realm. But what does the Metaverse concept encompass exactly? The term was coined by science fiction writer Neil Stevenson in 1992 in his novel Snow Crash. Aligned with Stevenson's initial vision, the Metaverse can be defined as a collective virtual open space, created by the convergence of virtually enhanced physical and digital realities [REF22]. It is thus an independent virtual reality, enabled by digital currencies and nonfungible tokens (NFTs).

Most famous metaverses include **Decentraland**, The Sandbox, Meta Horizon Worlds (Facebook) or **Cryptovoxel**, all of which are virtual reality spaces where users can create content, impersonate an avatar, buy land, organise events, play games, and more generally interact with one another. In principle, there is supposed to be only one Metaverse that equals a collection of different virtual spaces. For example, one virtual space might represent **Decentraland's** virtual world while another may embody The Sandbox's virtual reality. This collection of virtual worlds is jointly called the Metaverse.

As with every interaction in the physical world, interaction in the Metaverse needs to be linked to a digital identity of some sort. The Metaverse specifically led to the management of one user's avatar identity which is most often always disconnected from the state-issued identity. This can generally be done by using a crypto wallet such as Metamask. Crypto wallets store secret keys used to digitally sign transactions for blockchain distributed ledgers and are used as a keeper of cryptocurrencies or digital assets and NFTs. In a wallet, you can, for instance, find components of an avatar identity, such as gaming preferences and NFTs representing the avatar's username, its virtual clothes, or even the piece of virtual land he owns.

However, some metaverse iterations involve integration between one avatar's identity and one user's state-issued identity. This is especially true for corporate identity management. How to ensure, for instance, that the Samsung digital store recently opened in **Decentraland** is effectively owned by the eponymous South Korean company? One can also envision the rise of use cases that would require by law strong user authentication. In these cases, a bridge between these identities appears necessary to reconcile the physical and the virtual world. More generally, digital trust requires a persona identity to be backed by a real person identity for users to know with whom they are interacting, being business or individual. If the Metaverse is still in its infancy, functional and official identification in the Metaverse will surely be one of the coming years' hot topics in the field of digital identity.

NB: This subject is presented for illustration as a prospective case study, there may be questions or various interpretations to its future.

Key learnings: a review and summary

In this whitepaper, SIA has outlined the strategic and tactical challenges together with some of the key trends and technologies currently helping to shape the future of digital identity. The following quick review provides a summary of the topics explored in this paper:

- **The growing need for interoperability** is driving huge developments in protocols and standards around digital identity worldwide, including on data, API, biometrics, cryptography, cloud intelligence, and other key technologies. These efforts are focused on achieving alignments between countries/geographies as well as enabling greater alignment between public and private sector roles in digital identity ecosystems. New initiatives to achieve multi-stakeholders convergence or multi-countries governance frameworks area already underway.

- **The diversification of identity models means that governments need to go beyond just thinking about whether to choose a** centralised, federated, or decentralised model (such as self-sovereign identity). Instead, governments need to focus on building better user-centric ecosystems, utilising a mix of models that are best suited to a variety of different use-cases and technological environments.

- **The impact of the upsurge of electronic or digital wallet and mobile-based digital identity on the functional digital identity landscape is of great relevance.** Government and stakeholders need to prepare and develop adequate strategies to access digital services using identity wallets for a wide array of services and use cases. These include use case for health, mobility, financial KYC, payments, or digital money. In broader terms, all trusted interactions by citizens to access the public and private services the wallet can support.

- **Providing trusted retail digital finance for the wider public is an important emerging need** and digital identity is key for building digital trust. The evolution towards digital money, especially Central Bank Digital Money (CDBC), may need digital identity as a reliable link for accounts opening. It may enable the creation of special forms of identity which, together with the registry, guarantee the value of money as a personal money reserve and assure KYC and AML-CFT requirements in a fluid and trusted way (dependent on the amount and frequency of transactions).

- **The challenge of identity in virtual/ augmented reality needs to be addressed as** the emerging digital assets market ushers in new concepts around tokens as identifiers and references for valuation (e.g., non-fungible tokens for virtual art pieces). Blockchain registries are increasingly used as a valid reference to ownership for various kinds of virtual/hybrid assets. Web3, virtual reality, and gaming are generating new experiences that can cause confusion for users in relation to the degree and consequences of commitments taken in virtual environments. It is therefore important that clear distinction exists in the kind of digital identity that is used and to foster regulations and user education on the respective accountability and liability regimes that are applicable for both professionals and consumers markets. Special protocols that are clearly differentiated for virtual reality services will be important.

- **There are a number of critical tactical aspects that need to be addressed along the way**, such as *inclusion* challenges (rural inhabitants, elderly and disabled people, digital literacy), the continued *assessment of the user experience*, ensuring that *authentication and authorisation processes are differentiated* and clear to users, *user privacy* when there is cross sectoral use within a wallet, *interoperability* with other wallets and authentication of all transacting and trust parties, as well as the ability to include easy access to payment and digital money.

Conclusion and final takeaways

In conclusion, SIA provides some key pointers and recommendations for governments and project stakeholders:

- Make sure you analyse and understand evolving environmental factors, and create a monitoring tool for the elements you believe will have a direct impact on your digital services. Build an up-to-date policy and plan effective regulation updates for users in the most important social and economic situations.
- User privacy is paramount for today's citizens and consumers and there are now several models that give users greater control over their data. These solutions allow for the flexible and selective disclosure of identity attributes and electronic attestations sharing.
- Develop a use case assessment process to identify specific issues that could affect the development of trusted digital services. This will help support compliance and coherence as well as more efficient project development methods and an appropriate risk analysis tool
- Cross-state recognition and cross-border interoperability need to be considered early in the roadmap to digital services, identity ecosystems, and international cooperation. Electronic or digital wallets provide a new channel for digital interoperability, using appropriate standards.
- Address regulation and governance issues resulting from digital wallets and cross sectorial use. Support free choice between trusted solutions and offer alternative channels and credentials for digital identity.
- Adapt architecture models to use-case situations and users' requirements. Most often one size does not fit all; the most effective strategy is to test several models and achieve better maturity when selecting an architecture. Market expectations and business environment will likely be as important as technical outputs in terms of stimulating mass user adoption.

The SIA brings together a unique community of governments, NGOs, and other identity stakeholders and encourages best practice sharing between members and affiliates and frequently supports or organises workshops and networking encounters to facilitate this. Offering access to digital identity experts, SIA provides a variety of literature, online resources for methodologies and training practices – and more.

To find out more, make an inquiry, or discover how SIA can help propel your digital identity project forward, contact us via our website at https://secureidentityalliance.org/ or send us an e-mail at contact@secureidentityalliance.org

References

[REF1] Example of some definitions in standardisation bodies ITU 2010 Identity is the « representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context » in baseline Identity Management Terms and Definitions; ISO 2019 Identity is a set of attributes related to an entity in ISO/IEC 24760 Security and Privacy. A framework for identity management.

[REF2] Identification is about singling out or differentiating a particular entity, enrolment is about validating and registering the corresponding information. Sometimes the global process is known as “onboarding”; a term especially used in “Know Your Customer” and “Customer Relationship Management” business practices.

[REF3] This is most often in 2022 a password, combined with some second factor, which may be a physical token, binding to a mobile device, biometrics or (even discouraged due to the risk of breaches) a phone number where one-time passwords are sent.

[REF4] https://www.juniperresearch.com/press/digital-wallet-users-to-exceed-4-4-billion-by-2025

[REF5] https://worldpay.globalpaymentsreport.com/en

[REF6] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

[REF7] Pew Research Center, Americans’ complicated feelings about social media in an era of privacy concerns. March 2018

[REF8] International Cybersecurity Forum (ICF), Data Breach Barometer 2021. June 2021.

[REF9] See for instance CNIL https://www.cnil.fr/fr/appel-contributions-privacy-research-day-2022

[REF10] Proposal for a regulation of the European Parliament and of the Council amending Regulation EU 910/2014 (eIDAS) as regards establishing a framework for a European Digital Identity.

[REF11] Id. at recital 29.

[REF12] https://ecowas.int/

[REF13] https://www.eac.int/

[REF14] https://smartafrica.org/sas-project/digital-identity-for-africa/

[REF15] https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf

[REF16] It remains unclear if other governments, banks, and enterprises – particularly those located outside of the U.S. – will be quite so willing to hand over this power to a tech giant.

[REF17] https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guiding%20core%20principles%20for%20the%20development%20of%20a%20Digital%20Travel%20Credential%20%20%28DTC%29.PDF

[REF18] https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Visible%20Digital%20Seal%20for%20non-constrained%20environments%20%28VDS-NC%29.pdf

[REF19] https://www.w3.org/TR/did-core/

[REF20] https://www.w3.org/TR/vc-data-model/

[REF21] www.osia.io

[REF21] GARTNER, what is a Metaverse? https://www.gartner.com/en/articles/what-is-a-metaverse

Other reports by the Secure Identity Alliance:

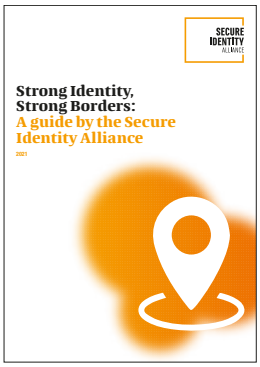
https://secureidentityalliance.org/ressources/publications

Giving Voice to Digital Identities Worldwide

Providing unprecedented 'on the ground' insights and perspectives, the study produced in partnership with onepoint gives a unique voice to stakeholders from 25 innovative sovereign digital identity schemes. Their shared learnings highlight the guiding principles and good practices that are critical for driving usage, adoption, and success – regardless of the digital identity model adopted.

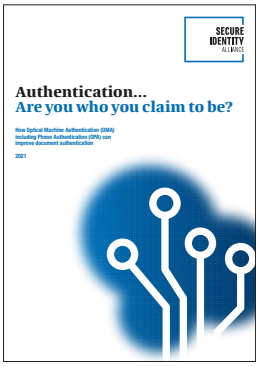
Passport Fraud Trends and Ways to Combat Them

The purpose of this report is to draw a clear link between the problems of document and identity fraud faced by issuing and control authorities, and selected private organisations such as financial services institutions. It also explores some of the technical solutions to those challenges as proposed by the global identity management industry.



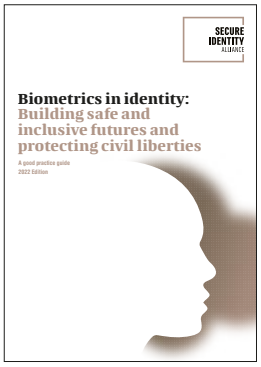
Strong Identity, Strong Borders

Looks at the need for border authorities to balance security and protection with efficient and frictionless passenger experiences. In addition to the major drivers shaping the future of the border control space, the report looks at the vital - and complex - role played by identity management, highlighting some of the evolutionary technologies incl. automation, biometrics, mobile, and bringing those solutions to life in the form of case studies from around the world.



Authentication: Are You Who You Claim to Be?

This report from the SIA addresses the challenge of identity authentication. Discussing the inherent difficulty in validating someone's identity, as well as some of the solutions that are currently available, the report also provides detailed use cases and recommendations for anyone who may be looking to improve their understanding of this critical practice.



Biometrics in identity: Building safe and inclusive futures and protecting civil liberties

There is no single 'right' way of building or operating a biometric system, but this toolkit is offered to those designing and running a system to help them consider important choices they need to make in order to build a biometric solution that meets their needs well while building safe and inclusive futures and protecting civil liberties

SECURE IDENTITY ALLIANCE