IDEMIA

Top Five Considerations for Building a National Digital ID Scheme

IDENTITY

POSTED ON 08.30.24

The United Nations is so convinced that universal legal identities will be a key factor in improving economic growth and the welfare of all citizens across the globe that it has set a goal of providing everyone on the planet with a legal identity by 2030.[1] To reach this target, the UN's ID2020 Alliance Manifesto believes the world needs the increased efficiency, scalability, and accessibility that only digital identity can provide.[2]

Where paper-based civil registry and ID systems exist, they are being transformed into digital and, where nothing is currently in place, the solution is being developed from the ground up. In reality, there are as many types of systems as there are countries, but here we take a look at the five key considerations for selecting and deploying a national digital ID program.

This report examines the five key considerations for selecting and deploying a national digital ID program.

Key Consideration 1: Ensuring Strong Laws, Regulations, and Standards Are in Place

Before considering the scope of the digital ID program in terms of systems and technology, a protective foundation needs to be built based on social, economic, and political factors. Obviously, these are domestic affairs for a country's government, but the legal framework of the country must be fully understood as it acts to protect everyone involved in the digital ID system.

Countries should enact specific laws governing the establishment, operation, and management of digital ID systems. These laws ensure that the system complies with national and international safeguards, such as the General Data Protection Regulation (GDPR) in the EU. These laws mandate stringent requirements for data security, consent, and individual rights for personal data.

Privacy and data protection regulations establish holder rights, consent requirements, and penalties for misuse. A key difference here between physical and digital systems is in the amount of personally identifiable information (PII) that is held. In the case of a physical ID, the PII made available to a third party for verification is the limited amount of data printed on an ID card or passport, if the chip of an electronic document is not read. By contrast, digital ID systems can carry much more information. PII and additional data about the holder is stored to facilitate the user experience in administrative tasks by digitally sharing trusted data and avoiding any typographical errors. However, this data is then potentially accessible to all kinds of service providers. Hence, it is crucial to put strong regulations in place regarding the consent-sharing rights of digital ID holders. The way the technical solution is built should obviously be compliant with the regulations but also ensure that it is based on a sole control and consent-only approach from the beginning. A mobile identity, for example, can be created in such a way that the holder can select only those specific personal

attributes, such as the holder being above a certain age, that are relevant for the one specific third party the holder is dealing with.

For an interoperable national ID system that integrates governments, service providers, and other stakeholders onto one platform, an additional layer of data exchange is needed to let one system send and receive data to/from another. Using open standards ensures that different systems and platforms can communicate and work together.

This way, users will go through the same processes, whether dealing with a domestic or foreign bank, telecom company, or other service provider, and can often avoid the inconvenience of having to re-enter data about themselves for each individual transaction.

But interoperability and modularity of the systems used is not just important for the interaction between the private and the public sector. Interoperable and modular systems, for both physical and digital ID management, are critical in driving competition between the providers, leading to innovation and, ultimately, more cost-efficiencies that the citizen can benefit from.

Case study—TelCo industry

The convergence of standards in the telecom industry has been vital for global interoperability and technological advancement.

It has ensured devices can communicate seamlessly across different networks and across geographical areas, significantly enhancing the user experience.

This convergence also enables the construction of operator networks using components from different manufacturers (e.g., Nokia, Ericsson, Huawei), as their solutions can interact seamlessly based on these standards. If an operator wants to change one of its suppliers, this is possible without impacting its entire network.

This standard harmonization and interoperability supported the rollout of 4G and 5G technologies, promoting consistent performance, reducing costs, and fostering innovation across the industry.

Key Consideration 2: Gaining Efficiency When Using the Existing Infrastructure

The decision as to whether to build a digital ID system from an existing physical one or to start from scratch is not as straightforward as it might first appear. Starting with an existing physical ID scheme and database certainly provides a foundation that can accelerate the development of a digital ID system, leveraging existing data and infrastructure. The provider's access to the so-called Root of Trust can bring additional benefits when setting up the digital ID scheme based on already existing databases. Many cases have proven that a provider's access to an existing database smooths the process of establishing the digital ID structure. The existing provider is familiar with the specifications of the system, as well as the regulatory framework of the country. This can significantly speed up the establishment of additional/adjacent systems such as those needed for a mobile ID, for example.

However, the necessary assessment of the existing infrastructure might uncover various physical ID systems, such as national identity, tax registration, voter ID, and medical cover, each serving different purposes and with its own database and procedures. These systems are often fragmented and lack a unified identity verification mechanism.

The Aadhaar system in India is a good example of how a pre-existing set of siloed physical identification methods was consolidated and transformed into a comprehensive digital ID system—all based on multiple biometrics that ensure the uniqueness of the identity stored.

In situations where there is little infrastructure for formal civil registration and identity management, it might be more practical to build the system from scratch. In these cases, stakeholder engagement is crucial in gathering input from government agencies, business, and citizen groups and defining the primary objectives, such as improving access to government services, enhancing security, and enabling digital transactions.

Case study—French electronic ID (eID)

The current French national eID card (CNIe), launched in 2021, enables French citizens to complete online transactions using their smartphone. Citizens receive an authentication request on their smartphone and the mobile app securely reads and authenticates the personal data held in the card's chip.

The digital ID system has a First Level security certificate from the French IT agency, ANSSI, so it complies with the EU eIDAS Regulation. The system will protect citizens' identity data and will ensure that only the authorized citizen has control over it.

Key Consideration 3: Choosing Leading Technology Based on Years of Innovation

Using technology appropriately and responsibly is essential in creating a modern digital identity scheme that is trusted by governments and citizens alike. The expertise required to achieve this is based on years of innovation and engineering experience at the cutting edge of identity management and secure documentation. It is not surprising, therefore, that only a few companies worldwide can demonstrate the know-how needed to pull together the streams of physical and digital technologies needed to design, build, and maintain a digital ID system.

Knowledge of technology and regulations
Leading a proof of concept with customers to prove their use cases and executing interoperability testing with other major actors of the industry are key actions in building foundations for the strongest technology in a national digital ID program.

Companies must consistently demonstrate industry foresight and financial commitment to R&D that ensures the proposed digital ID solutions remain current and compliant with evolving industry standards. Looking at the digital ID space over the past few years, focus had been on the implementation of the ISO/IEC 18013-5 standards but now, equally important, are OpenID4VC and OpenID4VCI, which will be important for the upcoming EU wallet implementation, as mandated by the amended eIDAS Regulation.

Fair algorithms
In the domain of national digital identity, biometric authentication is more reliable than other authentication techniques (e.g., PIN, password, token) and effectively improves access to public services and enables country digitalization. The implementation of such a system therefore triggers high expectations, which tend to render any potential technical error more difficult for the public to accept. It is important to be aware of this, have the appropriate processes in place, and make sure those operating the system know them well. For example, it is important to have a technology that is consistent across all ages, genders, skin colors, and ethnicities—in other words, to have fair biometric algorithms. For such systems, security is also paramount and must be based on years of innovations, as well as strong processes to design, develop, and test the products.

Future-proofing the solutions
In an era where technology evolves at a rapid pace, the need to future-proof digital ID schemes has become increasingly important. As smartphones receive frequent updates to enhance security and functionality, the eID cards, which digital ID schemes are often based on, must also adapt to stay ahead of emerging threats.

Typically, eID documents are valid for around ten years. During this period, fraud techniques evolve, potentially compromising the security of these documents. To counter this, it is essential for the operating system and applications within eID documents to be updatable, even after issuance. Upcoming regulations, such as those proposed in the EU Cybersecurity Act and the EU Cyber Resilience Act, mandate these evolutionary requirements to ensure continuous protection.

In the past, updating the operating system on an electronic ID card required reissuing the entire card, a process both time-consuming and costly. However, with innovative embedded software, the system can be updated on the fly. This then enhances, again, the security of the digital identity.

IDEMIA—Pioneer in mobile IDs

2015:
IDEMIA was the first company to pilot a mobile Driving License (mDL) in the US.

2017:
First digital ID to help secure state income tax returns.

2019:
First standards-based mDL in the US.

2024:

- First transatlantic DTC-1 pilot managed by IDEMIA
- 2 million mobile IDs to be issued in Colombia
- Go-live of mobile IDs for telecommunication operator
- Go-live of mobile IDs in Chile

Use case—System update on the fly

JPatch technology from IDEMIA Smart Identity facilitates remote upgrades of embedded software without compromising user data or privacy. The post issuance and credential management systems ensure that updates can be executed conveniently from any trusted location, eliminating the need for card replacements.

Personal and technical data such as certificates and PINs remain secure and unaffected during the upgrade process, maintaining the integrity and confidentiality of the information. This approach not only ensures the safety of the data but also streamlines the update process, avoiding the need for new card applications and reducing administrative burdens for issuing authorities.

Key Consideration 4: Securing Digital (and Physical) Identities with Biometrics

Biometrics are revolutionizing national ID programs, addressing some of the inefficiencies and vulnerabilities of traditional identification methods. By leveraging unique physiological or behavioral characteristics, biometrics offer enhanced security and improved accuracy in identification processes.

Biometric traits, such as fingerprints, iris patterns, and facial features, are nearly impossible to forge or steal, significantly reducing the risk of identity theft and fraud. Automated biometric systems also minimize human error, ensuring precise and reliable identification and authentication.

The efficiency and convenience of biometric identification are especially advantageous in large-scale national ID programs. A citizen only needs one account to access different public and private services, and it is not necessary to remember numerous passwords. Biometric systems streamline the verification process, making it faster and more user-friendly for both citizens and administrators.

Additionally, biometrics can enhance inclusion and accessibility by providing identification means for individuals who lack traditional documents, ensuring all citizens can access essential services and rights. The scalability and interoperability of biometric technology further enhance its appeal, as it can be easily expanded to accommodate growing populations and be integrated across various governmental and non-governmental systems.

Biometrics also help to improve access to public services and inclusion by being more reliable. This is because the error rate for authentication using biometric technologies is considerably lower than with techniques such as verifying a person's identity with the naked eye based on a photo in an identity document. In addition, biometric identification is more durable. If people lose their identification documents, they can use biometric verification to prove they are who they claim to be and ask for the documents to be reissued quickly.

A digital ID system without biometrics is almost unthinkable. The advancements in technology—for example, liveness detection with a smartphone—have been so enormous that biometrics, especially facial biometrics, are offering the most secure way of proving that the user of a certain mobile ID is really the holder of the underlying physical ID. For a potentially fully remote enrollment process, biometrics and multifactor authentication are the securest way to verify the authenticity of the individual.

Case study—Colombia's Cédula Digital

In 2018, the Colombian government officially launched its Digital Government policy. This national policy promotes digital inclusion and advanced technology implementation to consolidate a competitive, proactive, and innovative state and citizens that generate public value in an environment of digital trust.

At the end of 2020, a new physical and digital national ID card duo was launched to provide a high level of assurance in the digitization of public services.

The national digital transformation plan has been powered by the combined issuance of a new identity document and a mobile ID named Cédula Digital. The new Colombian identity card meets the highest security requirements on the market, supported by IDEMIA's LASINK™ technology to reinforce the security of the portrait and the document.

The new Colombian Cédula Digital, digital companion of the physical identity card, opens opportunities to securely grant citizens access to remote services and to allow in-person ID verification based on the latest industry standards in compliance with the Digital Government policy.

The Cédula Digital is assigned automatically from the moment the new identity card is provided to the citizen using biometric verification (fingerprints and face). Once citizens pick up their ID card in an official physical office, they receive an email with a QR activation code and a unique activation link. They can use either of them to activate their Cédula Digital using a biometric selfie check that confirms their identity, enabling multiple digital interactions.

Key Consideration 5: Collaborating Closely with the Private Sector

Just because a system has been launched, there is no guarantee that it will actually be used and adopted by all service providers. Government ID issuing authorities may mistakenly believe that service providers, from both public and private sectors, are following the development of a digital ID program, ready to jump into action as soon as it is deployed. If service providers and other relevant stakeholders are not involved from the outset in the design and rollout of the program, they may not show the level of support required for effective implementation and usage. Defining the

targeted advantages for citizens, as well as for the public and private sectors, ensures that the outcome of the project will be embraced by all parties and the project will therefore automatically be more successful.

Practical steps, such as technology suppliers and systems integrators providing “how-to” guides to support service providers in implementing the solution, can further enhance the collaboration, since some providers may not actually know how to begin implementing it.

Case study—Morocco

A best-practice example of involving stakeholders from the outset of a digital ID project comes from Morocco.

Before launching its national program, the country’s National Commission for the Protection of Personal Data carried out a study of around 100 service providers to understand how they consumed digital ID data. The findings of the study were then used to formulate personal data protection controls.

Today, after both physical ID cards and a digital platform have been deployed in Morocco, the system is having a positive impact on citizens’ day-to-day lives in terms of the ease of use of government and commercial services.

Choosing the Right Program Partner—Perhaps the Most Important Consideration of All

Establishing a national digital ID program involves multifaceted considerations and meticulous planning. By addressing risks of exclusion, setting up legal and privacy frameworks, aligning with international standards, and ensuring stakeholder involvement, countries can successfully deploy and sustain effective digital ID systems.

However, make no mistake, creating a country’s national digital ID system, whether from the ground up or from existing infrastructure, can be a daunting prospect. Established, experienced providers can offer crucial assistance in navigating such a large project. Their systems work 24/7 and are supported by competent teams worldwide that ensure highest availability of the service and continuous improvement and innovation. Choosing a partner to work with on the journey to creating a national digital ID program may be the most important consideration of all.

---

[1] https://unstats.un.org/legal-identity-agenda#:~:text=SDG%20Goal%2016.9%3A%20By%202030,a%20civil%20authority%2C%20by%20age

[2] https://www.id2020.org/assets/pdf/ID2020-Alliance-Manifesto.pdf

---