AWS INSTITUTE

Digital identity

The opportunity for government

Access Partnership

Introduction

Governments around the world are increasingly implementing digital identity (digital ID) systems to improve social services and promote innovation. The COVID-19 pandemic reinforced this trend and emphasized just how important it is that everyone be able to prove their identity online. This report aims to explore the strategic decisions underpinning successful implementations of digital ID systems. It draws practical insights for public sector leaders looking to steer their countries towards a well-designed and successful digital ID system, examining the successes and pitfalls others have encountered. In particular, the implementation of foundational digital ID, biometric-based authentication, and cloud-based infrastructure is emerging as best practice to help government navigate these challenges and maximize positive impact for their citizens.

The identity challenge

The Universal Declaration of Human Rights and International Covenant on Civil and Political Rights is clear: Everyone has the right to be recognized as a person before the law (United Nations General Assembly 1948; 1966). On top of this, everyday activities hinge on people being able to prove their identities. The United Nations defines legal identity as the basic characteristics (such as name, age, gender, date, and place of birth) conferred or recognized by a legally recognized authority. This is often done through registration and issuance of a certificate such as enrollment in a registry of births or other instruments of the civil registration system (United Nations Legal Identity Agenda).

It comes as no surprise then that the right to identity is featured in the United Nation's 2030 Agenda for Sustainable Development. Further to this, increasing the number of legally identified people is part of the Sustainable Development Goals (SDGs). In order to promote peaceful and inclusive societies, SDG 16.9 established the objective of providing legal identity for all by 2030.

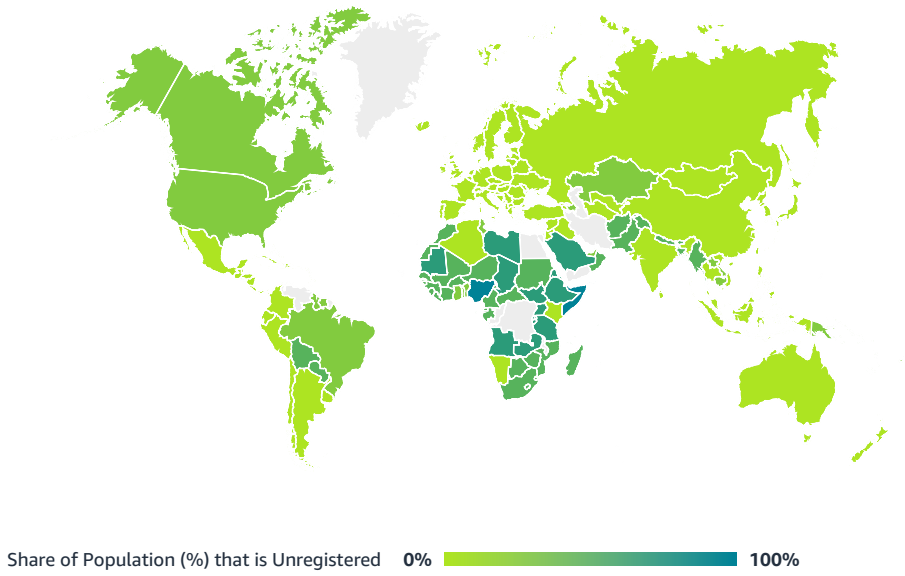
Although SDGs have catalyzed multi-stakeholder engagement since their approval in 2015, we are still far from achieving legal identification for all. Indeed, over half the world population may lack the ability to prove their identities online. The only indicator currently associated with SDG 16.9 refers to the proportion of children under five years whose births have been registered with a civil authority. This does not capture the full scope of the challenge. The World Bank's Identification for Development (ID4D) initiative attempts to go further and estimate the total number of individuals without a legal identity. The result is far from good. According to the most recent ID4D estimates, by 2018, one billion people globally did not have official proof of identity.

1:To address this methodological challenge, ID4D combined two different measurement strategies: (1) The Global ID4D Dataset, which is based on official figures from national ID authorities, voter registries, and UNICEF birth registration data; (2) Representative surveys from 99 countries, collected in partnership with the World Bank's Global Findex team. ID4D warns that neither of these is a perfect measure at the country level, but they provide a reasonable estimate regarding the scale of the global identity gap.

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Figure 1: Unregistered population share by country



According to the ID4D analysis, 81 percent of unregistered people live in Sub-Saharan Africa and South Asia. Sixty-three percent live in lower-middle-income economies and 28 percent in low-income economies (Desai, Diofasi, and Liu 2018). This makes clear that lack of identification is an acute problem for many of the poorest persons around the globe. It is also striking that in Sub-Saharan Africa, almost one in two people lack any form of legal identification. Furthermore, one in two women in low-income countries do not have an ID. The World Bank identifies refugees, stateless persons, people with disabilities, and people living in rural and remote areas as those who have the least access to identity documents (World Bank, 2019b).

Accelerated digital transformation—particularly development of citizen- and consumer-facing services via digital channels—heightens this challenge. As governments and private companies around the world digitize, individuals are required to not only prove their identities but to do so via digital channels. This is almost impossible for people without legal identification. However, it also affects individuals with identity documents that cannot be easily used digitally. On top of the billion people who do not have any legal form of identification, it is estimated that 3.4 billion people have an identification document but cannot use it online (McKinsey Global Institute, 2019).

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Digital ID systems

Public digital identity (ID) systems, underpinning the provision of legal identity to the population, can address both challenges, granting legal identities to use online.

A digital ID system can be defined as a personal identification system that uses digital technology to capture personal data defining a person's identity as well as providing for storage, management, and authentication protocols, which allow for a party receiving the digital ID to validate it during specific uses (World Bank, 2019a). By creating a unique digital ID, verifying that it corresponds to each person and their legal identity, digital ID systems guarantee these identities can be easily authenticated through digital channels to conduct specific transactions. Digital ID systems lead to multiple direct and indirect benefits. These include expanding public and private services to more people, increasing public services' transparency, efficiency, and agility, and boosting economic growth. Still, implementing digital ID also poses challenges related to data privacy and trust, security, and inclusion. This report argues that those challenges can and must be overcome through effective implementation.

Implementation requires confronting the multiple alternative models for digital ID systems, exploring different purposes, design choices, and operational characteristics that need to be considered when establishing a program's strategic direction. With no one-size-fits-all solution, different countries and public entities should be mindful of implementation contexts and desired outcomes when deciding on how to structure their digital ID systems.

This report further seeks to explore what defines a well-designed digital ID system and explores critical factors underlying its successful implementation. In particular, certain mindsets around data privacy and security must be confronted and debunked in order to provide a clear picture of how cloud-based digital ID systems can provide the speed, scale, and security needed for success. Drawing from the experiences of several countries, there are a number of high-level processes governments should strategically follow to establish and implement a well-designed system. Learn about some of the governance, technical, and policy considerations that support these processes.

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Chapter 1:
The opportunity of digital identity

Digital ID systems enable a government to do much more than simply issue identification documents. The benefits of digital ID systems go beyond enhancing legal compliance; they help make public and private services accessible to more people, act as a key innovation enabler, lead to higher transparency, and boost economic growth.

If implementation of digital ID was already important, it has become essential in the wake of COVID-19, which has sped up digital transformation worldwide. Many governments turned to digital channels to financially support households, organize COVID-19 testing programs, roll out vaccination plans, hold phone and video medical consultations, and transition education to online digital channels. These government services required people to digitally prove their identities in some form or another.

It comes as no surprise, then, that an increasing number of governments aim to start or expand their digital ID systems. In line with this trend, the Declaration of G20 digital ministers in August 2021 included for the first time 'inclusive digital identity' as a central component in economic recovery, development, and government transformation (G20 2021).

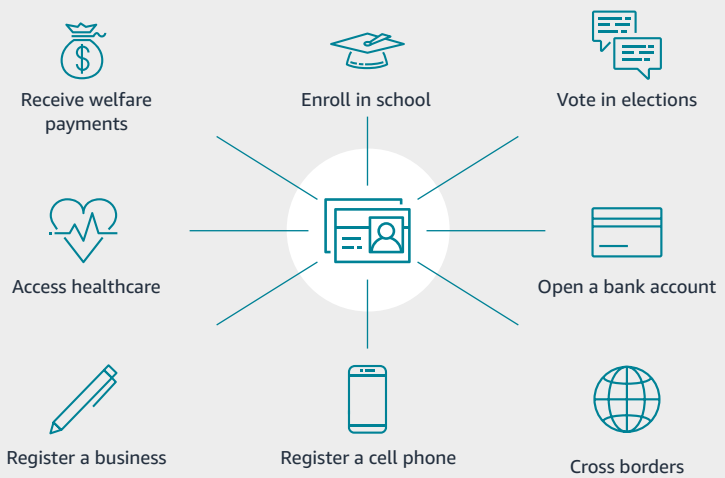
In collaboration with the OECD, the G20 has set up a mechanism for sharing digital identity best practice between G20 countries, acknowledging both the benefits these solutions bring, but also the challenges involved. In particular, digital ID systems present implementation challenges that are hard to solve under traditional paradigms, including issues such as privacy and trust, digital security, and inclusion.

Many practical implementation decisions associated with digital ID systems cannot be properly considered without exploring and understanding these benefits and challenges.

Benefit 1: Accessibility and Inclusion

Without a recognized form of identification, it is difficult to enroll in school, access social services, pass through border crossings, claim pensions and social welfare payments, open a bank account, obtain a mobile phone, present credentials for jobs and occupations, access healthcare services, vote in elections, or register businesses (World Bank, 2019b).

Figure 2: Systems that depend on personal identification



Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Digital ID systems allow for a simpler and more efficient implementation of all these services that hinge on personal identification, making them accessible to more individuals. A digital ID enables people to prove who they are with less friction, ensuring that their identity can be authenticated more quickly to access public and social services and used in a manner more secure against errors and accidental disclosures than more traditional methods of managing identity. As more individuals can prove their identities, the accessibility of services, opportunities for individuals, and opportunities for service innovation expand. Thus, a digital ID system can be a powerful equalizer, helping disadvantaged communities participate more fully in social, economic, and political life.

For these reasons, institutions such as the United States Agency for International Development (USAID) have argued that being able to digitally prove one's legal identity is crucial for development and inclusion (USAID 2017). Digital ID systems drastically enhance the capacity to extend public services to the poorest citizens of a country. For example, the Brookings Institution underscores that universal digital ID is the main enabler of universal cash transfers for economic relief and social support. In their opinion, "extreme poverty could be erased at a global cost of around $100 billion" through such cash transfers, but only if adequate digital ID systems were implemented (Bayuo and Tholstrup, 2021).

Cash transfers in Pakistan during the COVID-19 pandemic

The COVID-19 pandemic highlighted the need for well-functioning digital ID systems. In Sub-Saharan Africa and South Asia, many families face extreme poverty. Development specialists underscore that even experiencing poverty for a brief period of time can have a long-lasting impact (Kharas 2020). In this context, deploying cash transfers quickly to impoverished households has become an effective way to provide relief. Ultimately, countries with digital ID systems were in a much better position to implement them. This technological advantage allowed people to quickly prove who they were when applying for welfare schemes, and for governments to rapidly cross-check eligibility using different databases.

In Pakistan, the government introduced the Ehsaas Emergency Cash program in April 2020, with the target of providing 12 million families with approximately USD 75 each. Families could check through SMS messages whether they were eligible, which would have not been possible without the country's digital ID system. Data linked through the system such as registered property, travel history, and socioeconomic statistics were used to determine an individual or household's eligibility. According to government figures, the program has reached more than 15 million families and is an integral part of their efforts to tackle poverty across the country.

Tackling the implementation challenges

As a growing list of countries and governments acknowledge the benefits of digital identification, they are already taking steps to launch or advance their digital ID systems. Drawing from experts' opinions and case studies, the following chapters will help to strategically tackle the implementation challenges associated with digital ID systems.

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Benefit 2: Transparency, innovation, and agility

A digital ID system improves interaction between individual citizens and both public and private institutions. It is a critical building block for the design and improvement of more responsive, agile, and innovative services. In particular, it helps reduce operational costs, improve customer experiences, decrease turnaround times, increase delivery speed, and enhance security.

This impact on institutional efficiency is especially important in the public sector, where digital ID systems can strengthen transparency, efficiency, effectiveness, innovation, and the agile delivery of public services and programs (World Bank, 2019b). It is estimated that streamlined systems built on universal digital ID could save governments 110 billion hours of work, along with the associated reduction in expenditure (McKinsey Global Institute, 2019).

Reacting with agility to COVID-19: The South Korean case

South Korea has an integrated identity ecosystem linking a population register (resident registration, known as RR), a family register (family relationship registration, known as FRR), and the population change survey (PCS). Everyone in the RR has a unique Resident Identification Number (RIN) included in their national ID card, and nearly all government services require people to present their RIN (Joon Song et al. 2016). Since 2002, the South Korean government has brought these systems online, effectively building a digital ID system (Clark et al. 2018).

National ID and RIN numbers are integrated into the South Korean healthcare system, and the RIN is used as the foundational patient identifier. Furthermore, the integration between the healthcare system and Statistics Korea allows for seamless data collection and analysis (Joon Song et al. 2016).

This digital ID system, when facing the COVID-19 outbreak, enabled the South Korean government to rapidly deploy a comprehensive "test, trace, isolate" strategy. The government also had sophisticated data and statistics at hand to make public health decisions (Dighe et al. 2020). South Korea is frequently praised for the speed of its response, which would have been impossible without its digital ID system and its integration with healthcare.

Digital ID systems also significantly increase transparency and help reduce fraud in government-to-person transfers. When processing payments related to public wages, pensions, social welfare programs, unemployment benefits, child support, and conditional cash transfers, non-digital systems are vulnerable to both errors and corruption. A robust digital ID system makes impersonation more difficult and allows administrators to rule out ineligible candidates for a specific payment.

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Increasing public sector efficiency

Since their expansion in recent years, digital ID systems have reported extraordinary results in improving public services' efficiency and fostering transparency. In the Indian State of Andhra Pradesh, biometric smart cards helped reduce corruption, misallocation, and mismanagement of public funds (known as leakage) in social benefits payments by 10.8 percent. In Thailand, cross-checking beneficiaries of a cash transfer program against complementary government databases generated an estimated savings of between USD 29.7 and 59.4 million. In Uganda, verification of civil servants' identities against the national ID database led to the elimination of 4,664 ghost workers and saved USD 6.9 million (Clark, 2018).

Digital ID systems can greatly reduce administrative costs for government agencies as well as minimize fraud and errors. This, in turn, reduces costs in the citizen-government relationship and between government entities when cross-agency collaboration is needed. For example, utilizing a single digital ID system, one agency can request information on a specific individual from another agency quickly and seamlessly.

Particularly when adopting infrastructural and foundational approaches, governments can implement digital ID through a shared platform approach, building a unified system once that specific government agencies can reuse and leverage to create additional services without building their own system each time. Aside from budgetary and time-to-market benefits, this allows the public sector to eliminate redundant systems, and can help diminish unnecessary data collection. A unique digital ID presents enormous advantages in terms of data minimization, which means collecting the minimum amount of data needed to deliver a service. Whereas fragmented paper-based records across government departments will inevitably involve duplicated personal data, a digital ID system could link together data points housed across different agencies.

Estonia, one step ahead

Estonia has built a digital ecosystem where 99 percent of government services have moved online. This digital ecosystem's foundation is electronic identification (eID). Electronic identification (eID) is built into the Estonian identity card, which was first issued in 2002 and is a mandatory identity document for Estonian citizens. Besides regular identification purposes, the card can also be used to establish one's identity in electronic environments.

At present, 99 percent of Estonian residents are in possession of an identity card. According to the government, the ability to digitally sign documents saves the average Estonian five business days per year (e-Estonia 2017), and eID helps to save an estimated 2 percent of GDP each year by reducing identity-related transaction costs and facilitating online services (Clark, 2018). The Estonian digital ID system has also enabled the country's e-Residency program, which grants access to Estonian services for people who do not live in Estonia. More than 1,300 new companies have been created by e-Residents, bringing an additional $4.6 million into the Estonian economy (Lowmaster, 2018).

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Benefit 3: Economic growth

Digital ID systems enable a plethora of new and more efficient services, both public and private. For example, they can help allow more people to open bank accounts, make payments, and register businesses. This helps formalize previously unregistered financial interactions and promotes financial inclusion. Not only does this benefit individuals and communities, but also represents economic value for countries. In 2019, McKinsey reported that extending full digital ID coverage in emerging countries could unlock economic value of 6 percent of GDP by 2030 (McKinsey Global Institute, 2019).

Part of this positive effect is driven by private firms' use of the system (Lowmaster, 2018). The most effective digital ID systems provide not just a platform for government services but can also provide authentication services for private institutions, who may otherwise need to build their own means of authentication. In the first instance, firms leveraging digital ID systems can decrease expenditure by reducing administrative and transaction costs related to identity authentication, which is easier via digital means than paper. These systems can also help reduce fraud and slash compliance costs.

Digital ID systems can also be drivers of new revenue streams, as they enable firms to have a larger customer base within easy reach of services. As the number of people who can prove their identity increases, potential revenue opportunities also emerge. A staggering example of this is the potential revenue in financial services. It is estimated that 360 million people—a fifth of the unbanked population worldwide—cannot access financial services due to not being able to prove their identities (World Bank 2017). Finally, there is also a direct positive impact for new and existing private firms specialized in providing identity-related services.

Introducing Aadhaar, the largest ID system in the world

Aadhaar is the largest digital ID system in the world, with over 1.2 billion registrants, administered by the Unique Identification Authority of India (UIDAI). The program was launched in 2009 and centers on a 12-digit unique identity number linked to minimal demographic data and fingerprint and iris scans. Individuals are issued an unique ID number called Aadhaar which, after biometric deduplication, can be authenticated online using either biometric attributes or a registered mobile number.

Aadhaar allowed India to move from a slow, unreliable, and non-inclusive paper-based system to giving residents a unique and online verifiable identity. While Aadhaar is not a proof of citizenship, it has become mandatory for accessing many public services and welfare payments, with 99 percent of the adult population currently covered by the program.

Since its launch, Aadhaar had enabled the government to save approximately USD 12.4 billion in administrative costs (The Economic Times, 2018). However, this only includes direct savings and does not factor in the significant multiplier effect that the program has had across the Indian economy. According to June 2021 official data, 35-40 million authentications are carried out every day through Aadhaar, along with 4.3-5.5 million eKYC (electronic know your customer) procedures (Unique Identification Authority of India 2021). Since Aadhaar was implemented, the typical private firm's cost to onboard a new customer decreased by more than 99 percent, from approximately USD 23 to USD 0.15 (Lowmaster 2018).

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

On top of this, Aadhaar has transformed India's financial landscape. The Aadhaar Payment Bridge System, which uses the Aadhaar number as a central key for electronically transferring government benefits and subsidies to beneficiaries, processes, on average, 105 million transfers per month. This amounts to approximately USD 1 billion. More than 73 million banking transactions, mostly in rural areas, are carried out through the system per month, amounting to USD 2.5 billion.

Furthermore, the country is rapidly moving towards a remote, cashless, and paperless economy through IndiaStack. This is a set of APIs allowing governments and businesses to build on Aadhaar's foundational infrastructure. Monthly peer-to-peer transactions through Unified Payments Interface apps, powered by IndiaStack, amount to $45 billion monthly.

Implementation challenge 1: Privacy and trust

Digital ID systems hold personal datasets which may be considered sensitive or that individuals may not readily disclose to others. Additionally, the authentication processes associated with using digital ID systems could lead to the creation of authentication logs, whose metadata can be used for profiling and surveillance (Access Now, 2018).

This risk is heightened by the combination of biometric databases and facial recognition technology, which facilitates surveillance by authoritarian states (Solomon, 2018). The standards for data sharing between public agencies and law enforcement may create an additional concern, especially when expansive and ambiguous concepts of national security are deployed.

These concerns undermine public trust in digital ID systems. National histories and political cultures vary and may result in very different orientations of the public towards the government with regards to personal data. In many countries, citizens expect that the government has wide latitude to access and use data it possesses, such as for law enforcement. At the same time, in many other countries such access is strictly controlled and may be taboo. In a context where citizens fear governmental misuse of data, asking them to provide more personal information to the government may meet resistance, and uptake and implementation of digital ID systems will face head winds. As a result, robust data privacy frameworks will be a necessary component in some circumstances to build trust in the context of digital ID initiatives.

Aadhaar's legal challenges

Since it started in 2009, Aadhaar has been subject to repeated legal scrutiny by the Supreme Court of India. In September 2013, the Supreme Court issued an interim order stating that no person should suffer for failure to register with Aadhaar, and that the government could not deny a service to non-enrolled citizens. The Supreme Court ruling kept the scope of Aadhaar limited and stressed its voluntary nature. In 2017, the Court further ruled in a case stemming from Aadhaar that citizens have a fundamental right to privacy.

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

Despite placing these limitations on the system, the Supreme Court upheld the validity of Aadhaar in 2018 and affirmed that the system could continue to be used by the state, although it limited the use of biometric authentication by private companies. The court recognized that "the Aadhaar Act is a beneficial legislation which is aimed at empowering millions of people." However, the ruling also stated that "data protection and data safety" must be "ensured to avoid even the remote possibility of data profiling or data leakage." According to industry experts involved in developing Aadhaar, limiting the use of biometric authentication by private companies has curtailed the full potential of the Aadhaar system.

Implementation challenge 2: Security and misuse

Poor design of a digital ID system can place personal data at risk and foster the growth of cyberthreats. An effective framework for a digital ID system must be supported by an equally strong technical architecture and information security framework to safeguard data, as databases containing large amounts of personal information, including biometrics, are attractive targets for criminals. An additional challenge lies in the secure communication of data during authentication processes, especially when such systems are used for financial transactions.

As is true with privacy, ensuring trust in the security of digital ID systems is a challenge many countries face which can stretch resources and challenge the capabilities of even sophisticated countries without leveraging the expertise of more sophisticated technology partners such as with cloud technology. In October 2017, a security flaw was identified in the cryptographic keys associated with approximately 750,000 Estonian eID cards, which potentially allowed users' private keys to be inferred from public keys. The flaw left eID vulnerable to identity theft, with the country's prime minister quickly announcing that affected cards would be disabled until the problem was solved (e-Estonia, 2018). Similar design flaws can also open gaps which can be exploited for fraud and misuse. For example, Australia's myGovID, an app launched in 2019 aimed to allow users to establish their identity with Australian Government services. Original customer reviews quickly drew attention to poor security measures, such as how easily a person with fraudulent intent could register accounts using readily and commonly available information. Even though the system has been strengthened, security researchers have pointed to enduring flaws in the login process that could give unlawful access to personal accounts (Saarinen, 2020). The digital services overhaul of the MyGov ecosystem is set to cost USD 200 million. In order for digital identities to properly extend to digital health records, an additional USD 300 million will also be invested (Crowe, 2021).

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Implementation challenge 3: Inclusion

As argued before, digital ID systems can allow easier access to all services requiring proof of identity and foster inclusion. However, those without sufficient access to technology, especially the Internet, or with the physical capability or skills to make use of them, can be left outside the system.

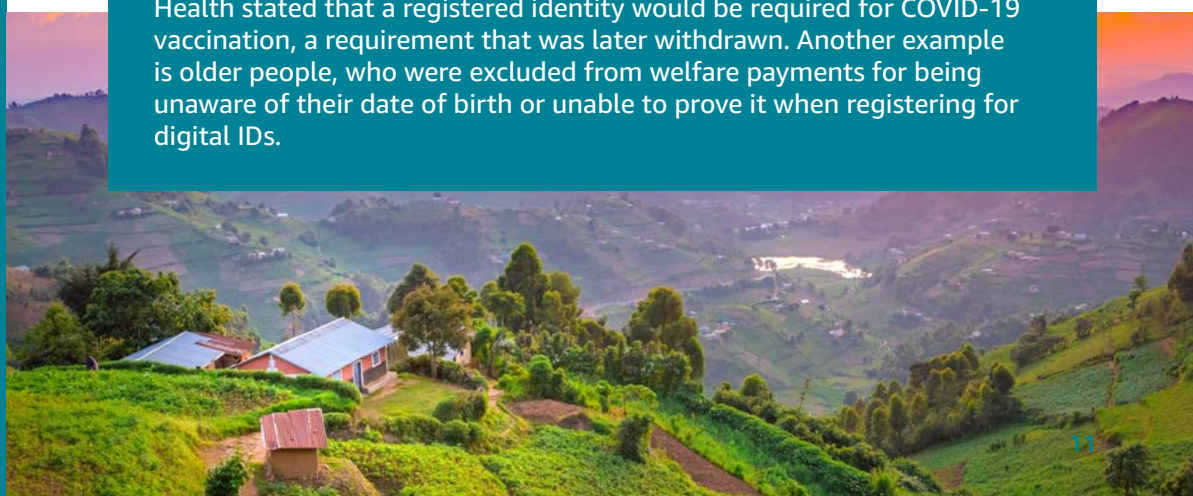
Digital ID systems are often based on biometrics. Even though it's a potentially powerful tool to quickly and easily extend access to many without special cards or devices, if poorly executed it can lead to the opposite effect and, in some cases, exclude certain segments of the population. Biometric identifiers such as fingerprints cannot always be captured or checked for older people, people with disabilities, or those who do intensive manual work. Undergoing an iris scan can be nearly impossible for people with involuntary movements (Privacy International, 2021). In India, for instance, there have been demands for Aadhaar enrolment centers to be accessible to the elderly and wheelchair users (Krishna 2018). Evidence indicates that, in certain cases, compulsory biometrics led to exclusion of some from public food distribution programs (Muralidharan, Niehaus, and Sukhtankar, 2020). Therefore, while rolling out a digital ID program, it is equally important to enable mechanisms that allow enrolment for exceptional cases. For example, Aadhaar has biometric exception provisions in its enrolment software to enable enrolment of residents with poor or no biometric. Similarly, when a digital ID system is being introduced in public service delivery, one should focus on overall process re-engineering and ensure mechanisms to extend service delivery to people who may not have either a digital ID or are unable to verify their identity digitally.

A digital ID system can also exclude those with fewer skills in using technology. When public and private services undergo a process of digital transformation, population subgroups less comfortable with digital channels could be unintentionally left behind. If this is left unaddressed, it can be have dire effects on the inclusion of the elderly, and it is also particularly damaging for gender equality; according to UNESCO and the EQUALS Coalition, women and girls are 25 percent less likely than men to know how to leverage digital technology for basic purposes (UNESCO and EQUALS Skills Coalition, 2019).

Digital ID challenges in Uganda

Uganda's digital ID system faced inclusion challenges in its initial biometric registration phase. Persons with disabilities were turned away from registration centers, as there were no alternatives to providing fingerprints. The severity of the problem was increased in many cases by long distances between registration centers and where many people lived, as well as the lack of application forms provided in local languages (Iyer, 2021).

A system that was non-inclusive led to direct exclusion in service delivery for groups that were already marginalized. Initially, the Ministry of Health stated that a registered identity would be required for COVID-19 vaccination, a requirement that was later withdrawn. Another example is older people, who were excluded from welfare payments for being unaware of their date of birth or unable to prove it when registering for digital IDs.



Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Chapter 2:
Digital ID structures

ID systems have historically been used by governments to provide individuals with official proof of identity. These systems collect identity attributes—such as name, address, date-of-birth, and fingerprints—and then validate them to establish an individual's identity. This validation is demonstrated through credentials like ID cards or unique identification numbers, which individuals can use as proof of identity when interacting with relying parties such as government agencies, financial institutions, or employers (World Bank 2019a).

As shown in the previous chapter, countries are increasingly deploying digital ID systems, which leverage digital technology throughout the identity lifecycle to increase access to and inclusion in identity-based services; improve the design, operation, and transparency of government services; and enable previously untapped economic growth.

Digital ID systems are being used strategically to either modernize existing paper-based systems or establish brand new identity systems; they are particularly being leveraged by countries that do not have any established or reliable ID systems to leapfrog traditional models. These systems enable digital verification of their identity, ensuring that their digital identity corresponds to their actual identity and authentication—matching of their unique identifier—for a wide range of in-person, online, and remote transactions (World Bank ID4D Event 2021).

A successful digital ID system must have a strategic direction developed by governments in tandem with relevant public and private stakeholders. This common vision must guide decisions regarding the structure and implementation of a digital ID system and includes key decisions such as its purpose, use cases, and design, which are discussed in more detail below. Decisions on these aspects are strategic and vital to ensure that the design of a digital ID system is contextually and situationally appropriate.

Purpose of identity systems

All identity systems have either a foundational or functional purpose (GSMA 2018). Foundational systems are established and operated by governments to provide identity to the general population as a general purpose public good available and accessible to all, which is then verified through credentials such as national IDs. These foundational identity credentials, the creation and permissible use of which is usually provided for under law, are used in a wide variety of government and commercial transactions. Conversely, functional systems can be established and operated by either governments or private institutions to provide identity to a subset of a population for delivery of specific services (World Bank 2019a).

A single person may have a wide variety of functional IDs for different use cases such as confirming eligibility to drive a car or provide proof of insurance. Even though these may in some cases be leveraged as a public good by other parties for authentication purposes not originally envisioned, they are generally linked legally or operationally to a particular use case and may not serve for general purpose identification in all circumstances. Foundational and functional systems enable governments to pursue different use cases and serve different parts of the population, as well as utilize different operational practices and eligibility requirements (GSMA 2018; World Bank 2019a)

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Figure 3: Foundational Systems

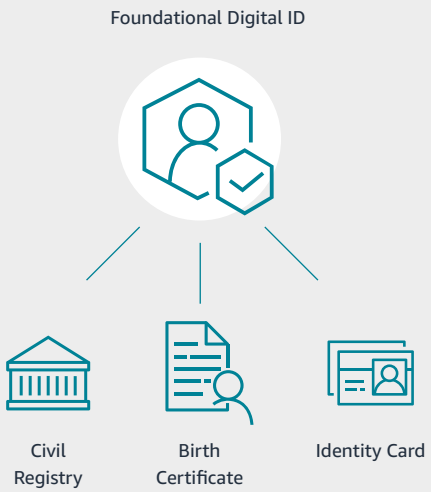
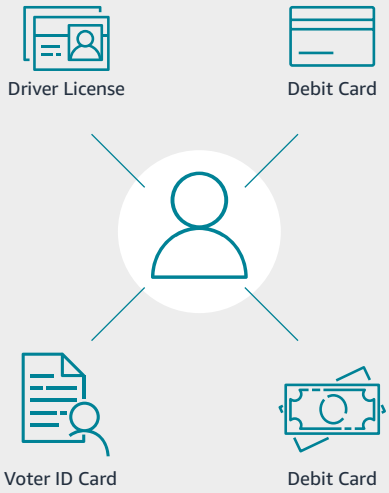


Figure 4: Functional Systems



Peru's RENIEC sets the standard for foundational systems

The National Registry of Identification and Civil Status (RENIEC) is an autonomous constitutional body that maintains a centralized civil registry of all Peruvian citizens and distributes the National Identity Document (DNI), which is the only personal identity card recognized by the government. The card is used for civil, commercial, administrative, and judicial purposes such as voting, accessing eGovernment services, and engaging with private services such as banking and healthcare.

These IDs were traditionally paper-based. However, this existing national system is now serving as the base for physical cards with cryptographic chips (DNI-e) that provide electronic signature, smart card, and biometric authentication functionality (Reuben and Palacios 2018).

United States' state-issued driver licenses steer broad use of functional systems

Individual US states issue driver licenses that are used to verify an individual's eligibility to drive a car. These IDs, which are paper-based but slowly transitioning towards digital versions, are distributed to individuals once they pass requirements such as driving tests. They include facial images as well as biometric (i.e., height) and demographic (i.e., age) data.

Although the primary purpose of these IDs is to regulate the use of cars, they are also used for general identity verification; for example, Americans use driver licenses to prove their identity when traveling domestically and conduct age verification when making age-restricted purchases. The use of functional IDs as de facto proof of identity for uses beyond their intended scope is common in countries that lack foundational ID systems (World Bank 2019a).

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

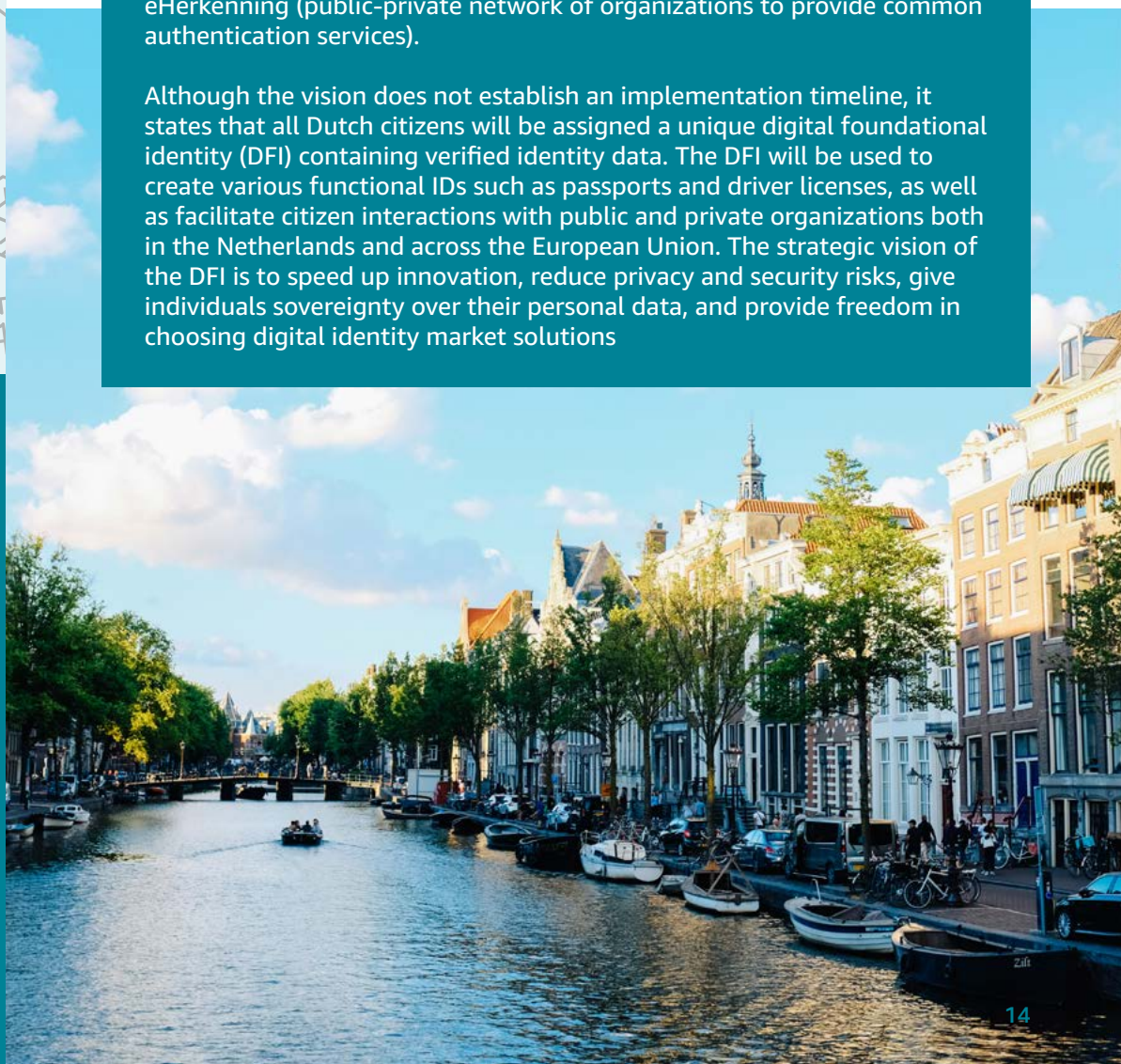
Foundational and functional ID systems collectively make up a country or region's larger identity ecosystem, where different systems can function either separately or together in a single jurisdiction for a variety of use cases. For example, Peru's DNI or DNI-e provide citizens with official proof of identity that can be used in all scenarios where identity verification and authentication are required; the country's government then utilizes this DNI to provide complementary functional IDs such as driver licenses to provide niche or add-on services that are not applicable to an entire population. In other countries, one or a set of functional IDs—such as a driver license, birth registry, or tax number—may be widely accepted throughout the identity ecosystem in the absence of a single foundational ID.

Therefore, a first strategic choice lies in whether a foundational or functional ID system is being pursued. Ultimately, a foundational system guarantees that a government is issuing a legal identity that can serve as a strong basis for additional public or private services

The Netherlands establishes a strategic vision for foundational digital identity infrastructure

In early 2021, the Dutch State Secretary for the Interior and Kingdom Relations, Raymond Knops, published his vision for the government to facilitate a streamlined and reliable national digital identity infrastructure for use by both citizens and organizations. The country currently has two different voluntary national digital identity systems: DigiD (public digital identity for citizens to interact with the government) and eHerkenning (public-private network of organizations to provide common authentication services).

Although the vision does not establish an implementation timeline, it states that all Dutch citizens will be assigned a unique digital foundational identity (DFI) containing verified identity data. The DFI will be used to create various functional IDs such as passports and driver licenses, as well as facilitate citizen interactions with public and private organizations both in the Netherlands and across the European Union. The strategic vision of the DFI is to speed up innovation, reduce privacy and security risks, give individuals sovereignty over their personal data, and provide freedom in choosing digital identity market solutions



Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Design of identity systems

Implementing both paper-based and digital ID systems requires making several design and technical choices throughout the ideation, development, and operation phases that are vital to helping ID systems achieve their intended purpose.

For example, administrators setting up an ID system must determine how to establish proof of identity credentials and what protocols are necessary to confirm that the person presenting themselves indeed corresponds to the ID presented. Likewise, they must also determine what information will be collected to verify identities; possible options include inherent information like biometric parameters, accumulated information like individual preferences, or assigned information like national identity numbers.

Figure 5: Types of personal information

Inherent
Intrinsic to an individual

- Date of Birth
- Fingerprints
- Facial geometry
- Iris/retina scan

Accumulated
Developed over time and may evolve

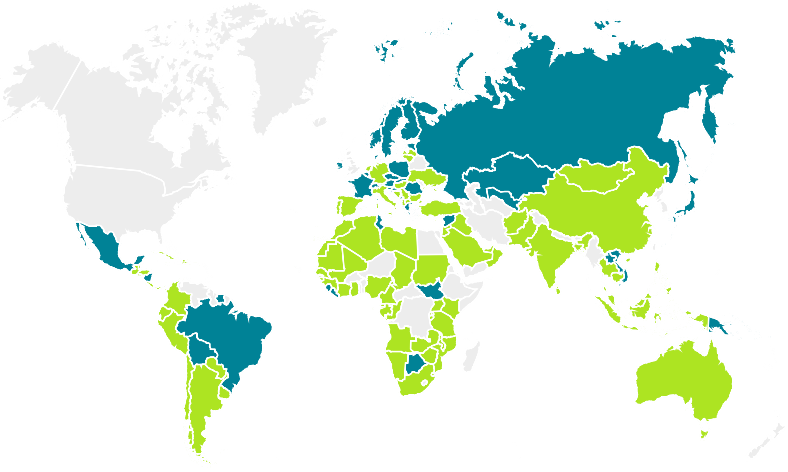
- Preferences
- Behaviors
- Address
- Transaction history

Assigned
Related to an individual, not intrinsic

- National identification number
- Tax or social security number
- Telephone number
- Email address

Selecting the types of data that will be tied to digital identity is a second strategic decision. Certain attributes enable specific transactions better than others, and a system's use cases influence the choice of attributes (World Economic Forum 2016). Regardless, systems should aim to minimize attribute collection and storage to the minimum that is necessary to validate identity. And globally, an increasing number of countries are choosing biometrics to authenticate personal identities.

Figure 6: Countries with digitized ID systems



Digitized ID system; Fingerprint and/or iris biometrics
Digitized ID system; No biometrics

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

The rise of advanced biometrics

As countries weigh different design elements, one increasingly common choice is the use of biometrics for identity authentication. Use of these parameters, including fingerprints, iris scans, or facial geometry, carries several benefits.

1. They are intrinsic to individuals and unique, which, though always important, is especially so in countries with large populations.
2. They provide multiple alternative attributes, which is important to include individuals that may not have specific types of biometric attributes (i.e., fingerprints, irises, facial imprints).
3. They are lower cost and are easily integrated into daily life, especially with increasing mobile penetration, which is important to increase the feasibility and usage of a digital ID system.
4. They do not require individuals to use or carry specific devices, credentials, or tokens that could be lost, which is especially important in countries with less wealthy or more transient populations.
5. They do not require governments to deploy or maintain specific and dedicated hardware systems, which is important to increase convenience and longevity of digital ID systems and avoid vendor lock-in.

However, the use of biometrics may have drawbacks. Biometric data has heightened privacy risks due to its sensitive nature and, even though more secure than some identity technologies, stored biometric data may need additional cybersecurity guardrails. Additionally, use of special equipment may be required to gather or measure some biometric attributes, which can create logistical and inclusion challenges for delivering services to all segments of a population such as those in rural areas or with disabilities.

Furthermore, some communities may distrust biometric data capture due to perceived potential for surveillance or social or cultural stigmas. Like other design choices, governments should evaluate all attributes for identity authentication (including biometrics) and choose one that best matches their systems' purpose and cultural and social context.

As countries confront these individual design and technical choices, they can also evaluate them on a spectrum from instrumental to infrastructural approaches. Instrumental approaches are highly use case driven and reliant on unique standards or proprietary technology, whereas infrastructural ones are compatible with multiple use cases and leverage common standards and open-source technology (USAID 2017).

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Instrumental approaches

- Purpose limited to a single identity use case or initiative
- Design, implementation, and phase-out driven by project time frame
- Dependent on custom software, hardware, and data standards

Infrastructural approaches

- Built with long-term objective
- Utilize open-source platforms and open standards
- Can repurpose for other use cases with minimal additional resources
- Designed and implemented with local stakeholders

Integrated Nutrition
(South Asia)

- Functional ID system to track beneficiaries of nutrition projects.
- Relied on proprietary software and nonstandard geocodes.

National ID
(Nigeria)

- Foundational national ID system
- Relied on proprietary systems from private vendors that limited reuse

Simprints
(USAID)

- Functional biometric health record system to monitor maternal health
- Utilizes open standards for multiple digital platforms

NADRA
(Pakistan)

- Foundational biometric national ID database
- Utilizes common data and technical standards
- Utilizes mobile and women-only enrolment teams to include hard-to-reach populations

Foundational and functional systems can incorporate elements of both instrumental and infrastructural approaches. However, approaches that fall along the infrastructural side of the spectrum tend to contribute more to countries seeking to create a cohesive and sustainable ID systems, whereas instrumental approaches must be put into the proper context, and can be inefficient, and ignore social, political, and economic aspects that are essential for system success (USAID 2017).

Instrumental approaches to digital ID systems can create challenges such as government agencies with proprietary siloed systems and the lack of a common trust framework across public and private identity stakeholders within the larger identity ecosystem (World Bank ID4D Event 2021). These challenges lead to larger scale waste and significant opportunity cost.

Contents

› **Introduction**

› Chapter 1:
The opportunity of digital identity

› Chapter 2:
Digital ID structures

› Chapter 3:
Designing an effective digital ID system

› Chapter 4:
Lessons learned and best practices

› **Bibliography**

Pitfalls to avoid when designing tech-drive ID systems

- Exclusion of vulnerable communities such as rural, low income, marginalized, or disabled populations that may not have access to costly infrastructure or have lower capacity to engage with high-tech systems
- Vendor lock-in and dependency that can reduce flexibility of a system to grow, prevent system re-use and evolution, and create greater costs to switch between vendors or proprietary technologies
- Frequent and necessary system maintenance and upgrades to keep the system functional and secure
- Fragmentation of ID systems in the same identity ecosystem due to potential technology or standards incompatibility

Governments should deploy digital ID systems that are not dependent on specific types of technology, modified to fit local conditions and contexts, and comply with interoperable practices and open standards for identity. These conditions are necessary to create dynamic and cohesive ID systems that can respond to rapidly evolving technologies, as well as prevent information fragmentation between different ID systems within identity environments.

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Operation of digital identity ecosystems

As countries implement new digital ID systems and digitize legacy paper ones, the identity ecosystem they operate within becomes more complex. Digital ID systems incorporate a wider range of actors with more diverse responsibilities, interests, and priorities than traditional paper-based ones (World Bank 2016).

This complexity has created new models that countries, regions, and private entities utilize to establish, operate, and manage digital ID systems. Several considerations may impact the implementation approach chosen, such as systems and actors already present in the existing ID ecosystem and the needs of specific stakeholder in the implementing country, region, or entity. It is also possible to implement hybrid models that incorporate elements of two or more models (McKinsey Global Institute 2019).

Centralized Ecosystem Model	
What is it?	One public entity provides a centralized government-driven digital ID system (World Bank 2016), where it operates and manages a central repository of individuals' identities. The public entity acts as an identity provider by authenticating individuals' identities and providing attributes to relying parties.
How is it best used?	The system provides a single source of truth for a complete and standardized view of individuals' identities, as well as streamlining access to critical online government services.
What is the role of the public sector?	This model is government-driven, where the public sector acts as both the regulator of the identity ecosystem as well as the identity provider by establishing a centralized national repository.
What is the role of the private sector?	This model does not carve out a large role for the private sector in the collection, verification, or authentication of identity. However, companies may support the technical implementation or deployment of the centralized identity repository and system (i.e., provisioning of software or hardware).
What are its advantages?	• Provides a legal identity • Streamlines service delivery • Leverages government presence throughout territory • Leverages existing government initiatives • Enables direct government control over whole system • Creates consistent ID services and experiences
What are its disadvantages?	• May not fully leverage third parties' (i.e., financial institutions) experience in managing digital identity • Requires strong buy-in from the government agency ecosystem • Concentrates risks and liabilities, creating a single point of failure
Where has it been used?	Aadhaar (India), NADRA (Pakistan), NIDA (Rwanda), PhilID (Philippines), RENAPER (Argentina), RENIEC (Peru)

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

Federated Ecosystem Model	
What is it?	Multiple public or private entities provide a government recognized digital ID system that is accredited through a trust framework or federation authority. A central identity provider operates and manages a central repository of individuals' identities. Other identity providers (or, brokers) authenticate individuals' identities against this repository and provide attributes to relying parties.
How is it best used?	Providing a single source of truth for a complete and standardized view of individuals' identities, as well as streamlining access to online government and commercial services by eliminating proprietary logins through third-party authentication.
What is the role of the public sector?	This model is mostly government-driven, where the public sector acts as both the regulator of the identity ecosystem as well as the central identity provider through an established centralized national repository. Individual public entities can also act as identity brokers.
What is the role of the private sector?	This model enables the private sector to serve in an identity broker capacity. Additionally, private entities may support the technical implementation or deployment of the centralized identity repository (i.e., provisioning of software or hardware).
What are its advantages?	• Simplifies integration of multiple identity providers with relying parties • Enables privacy by creating greater distance between relying parties and source data • Distributes cost of system creation, operation, and maintenance across multiple identity providers • Reduces potential for abuse of centralized repository or system • Widens range of institutions for individuals to choose from to provide identity
What are its disadvantages?	• Requires coordinated decision making between multiple public and private entities • Creates complexity that may disincentivize entities from participating as identity providers (i.e., legal agreements, technology, and data management standards)
Where has it been used?	BankID (Norway), BankID (Sweden), GOV.UK Verify (UK), Itsme (Belgium), NemID (Denmark), TUPAS (Finland)

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

Open Market Ecosystem Model	
What is it?	Multiple public or private entities provide a composite identity that is based on other functional ID systems or civil registers. Identity providers operate on bilateral agreements with individual public or private entities rather than through a central brokered scheme. This model may or may not employ self-regulation frameworks.
How is it best used?	Providing a private sector-driven identity market where entities already have expertise in creating, utilizing, and managing digital identities. This system is best suited to developed countries that already have established national identification processes and high birth registration rates.
What is the role of the public sector?	This model does not establish a centralized national repository, but individual public entities may act as regulators or identity providers.
What is the role of the private sector?	This model enables the private sector to serve in self-regulatory or identity provider capacities.
What are its advantages?	• Minimizes potential for misuse or manipulation of a centralized national repository • Enhances user control of their identities and transactions • Enables private sector to innovate new identity solutions to access online government and commercial services in a secure and efficient manner
What are its disadvantages?	• Potentially created duplicated identities • Potentially does not provide government recognized national identification or legal identity • High level of effort may be needed to implement standards and protocols that enable widespread online verification of IDs
Where has it been used?	Government Sign-In by Verified.Me (formerly SecureKey Concierge) (Canada), National Strategy for Trusted Identities in Cyberspace (NSTIC) (US)

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

Decentralized Ecosystem Model	
What is it?	Individuals choose their own digital identity attributes that are shared directly with relying parties. This model is enabled by distributed ledger technologies such as blockchain that can establish, manage, and share identity among different entities.
How is it best used?	Incorporating many identity providers (individuals) and relying parties, as well as ensuring individuals' convenience, control, and privacy online by allowing them to choose which relying parties hold their information. This system is also best suited to developing a full digital economy that requires multiple connections between entities to enable government and commercial service transactions.
What is the role of the public sector?	This model does not establish a centralized national repository, but individual public entities may act as regulators or identity providers.
What is the role of the private sector?	This model's use and adoption is currently driven by large internet platforms, software providers, and cloud service providers. Additionally, companies may support the technical implementation or deployment of the decentralized system (i.e., provisioning of software or hardware).
What are its advantages?	• Minimizes potential for misuse or manipulation of a centralized national repository • Enhances user control of their identities and transactions • Prevents single points of failure
What are its disadvantages?	• Requires a strong and well-developed foundational ID system to substantiate self-assigned identity • Potentially does not provide government recognized national identification or legal identity • Minimizes ability for individuals to raise problems or grievances without a central authority • Relies on emerging infrastructure (blockchain) that is not mature enough for scaling identity services • Relies on high cost and energy consumptive infrastructure
Where has it been used?	National Health Service Pilot (UK)

Each identity ecosystem model provides its own advantages and disadvantages. However, individual countries, regions, and entities must evaluate the current state of their ID ecosystem, the needs of their stakeholders, and determine the purpose of their system when selecting an ecosystem model and implementation approach (including design and technical choices). Entities need to make many contextual determinations such as whether to leverage any pre-existing identity programs, how much to involve the private sector, and how to gain public buy in.

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

Challenges that guided Aadhaar's design decisions

When designing and implementing the Aadhaar digital ID system, the Indian government had to make several difficult decisions about how to create a cohesive and resilient identity ecosystem.

The government decided to synchronize fragmented identity efforts in 2009. It established the Unique Identification Authority of India (UIDAI) and gave it a budget to create and manage a centralized national repository of all Indian residents and citizens. Aadhaar was envisioned as a unique biometric ID for the entire population. Biometric attributes such as fingerprints and iris recognition were selected because of the large size of India's population, where multiple individuals may have overlapping personal information, and frequent variations in the spelling of a person's name. Likewise, biometric attributes were chosen because they were static and would stay constant across a person's lifetime.

It was clear from early on that a centralized ID model was necessary for Aadhaar to be successful because of the constant flow of people across Indian states; federated or state-level models would not be able to establish common IDs that could work across the nation for migratory populations. At the same time, the scale of the system and its potential application, the need to ensure inclusive coverage of a diverse population, and the need to deploy quickly pushed designers towards an open, interoperable, and flexible system. To achieve this, UIDAI was able to use the backing of the national government to gain support from other federal and state-level agencies, as well as private entities. UIDAI translated this support into a large ecosystem of public and private entities who helped to register individuals for Aadhaar, leveraging individuals' relationships with local governments and businesses into broader public trust in and rapid uptake of Aadhaar, enrolling 1 million new persons per day at peak enrolment.

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Future structures of digital ID systems

Even as countries, regions, and private entities are investing in and building out digital ID systems, technology is evolving at a rapid pace, changing digital ID systems' design and implementation. Most importantly, technology is enabling new ways to use an individual's information and behavior to establish trust in their identity. For example, advanced biometrics are creating stronger verification and authentication methods and distributed ledger technology is strengthening the protection and integrity of information.

Additionally, evolving concepts of digital identity are presenting new ways for identity to be collected and validated. For example, the European Union's Electronic Identification and Trust Services (eIDAS) Regulation promotes cross-border ID systems that are provided through supranational and regional organizations. These advancements and the resultant digital ID frameworks will continue to disrupt traditional ID systems and models.

Figure 7: Future structures of digital ID systems

Advanced Biometrics
Physical traits as identity attributes will increase as identification kits become more accessible and technologies enable collection and verification of niche biometrics such as voice. This data could identify those currently excluded or undeserved by existing systems

Self-Sovereign Identity
Individuals will own their identities as distributed ledger technologies become mainstream and countries strengthen foundational systems for identity verification. This type of model places individuals in control of identity transactions.

Supranational Systems
As movement across border continues to increase, it will be valuable to have a digital ID system that is globally recognized and based on common standards. This type of system could increase trade and promote safe migration.

As new technologies develop and the number of digital ID systems around the world continues to expand, best practices continue to evolve. To meet the needs of the moment, governments need to critically examine these so that they can move with the speed necessary to leverage the benefits of digital ID systems. Drawing from how some jurisdictions have successfully overcome challenges and how others became cautionary tales, the next chapter will explore how some of these lessons learned should shift mindsets to speed adoption of the most successful cloud-based approaches.

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Chapter 3: Designing an effective digital ID system

When making the decisions needed to set up a digital ID system, countries start with an array of elements and capabilities already in place, and they may seek to emphasize different goals and use cases of digital ID more than others. Nonetheless, successful strategies focus on making the choices that best enable a new digital ID system to:

- Be capable of uniquely identifying individuals and ensuring that only an individual can create and control their identity
- Provide reliable authentication robust enough for the intended purposes of the public sector as well as for the private sector
- Ensure inclusion of all strata of society, especially underprivileged or marginalized groups
- Be adequately secured and trustable to ensure confidence in the privacy of any information it contains
- Provide individuals with the information and choice they need to feel empowered
- Be nimble, scalable, adaptable, and future-proofed to adopt to technological advancement and new use cases beyond what was originally envisioned

There is no single model of the right digital ID system that will be appropriate to every context to achieve these ends. But there are many common challenges for governments and the stakes are high. First, the technical architecture of the system must be suitable. Whatever the deployment model, implementing digital ID requires significant infrastructure which must be appropriate in scale to the system and population served, both at launch and for anticipated future uses. It must also be designed to operate in a manner consistent with system needs, including managing large and fluctuating numbers of incoming authentication requests.

Second, significant efforts must go into protecting data. Personal data that is processed by the system must be appropriately governed with law, regulation, and policy as well as protected with technical and organizational measures in order to be compliant with the law and engender trust. In the face of constantly evolving security threats and technological capabilities, this is no easy task for any organization, including governments.

Third, the project must be effectively managed throughout its lifecycle. As with any complex government IT-enabled project, building and managing this infrastructure is complex, and opens many opportunities for poor design decisions, implementation problems, and operational errors to add unforeseen difficulty and expense. These risks only become greater the longer a system has been in place, as technology ages and becomes out of step with the larger technology ecosystem, new vulnerabilities are found or created, and use cases and user expectations evolve. When serving the population at large, it may only take a few problems to seriously undermine public confidence.

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

Maximizing benefits with cloud computing

To manage these and other challenges better, cloud computing has emerged as a critical factor that enables success of digital ID systems, and is increasingly being considered by countries and governments globally.

Cloud computing is a service-based model of information technology (IT) consumption. Cloud service providers (CSPs) provide ubiquitous, convenient, and on demand network access to a pool of configurable computing resources (including networks, servers, storage, applications, and services). These can be rapidly provisioned and released with minimum management effort or interaction with the service provider. CSPs may provide services to customers within three deployment models: on premises infrastructure which is provisioned for the exclusive use of a single organization either on or off the premises of the organization; public cloud infrastructure which is able to be provisioned for the general public; community cloud which is provisioned for the exclusive use of a class of users from multiple organizations; or a hybrid combining features of the above (Mell and Grance).

In general, the cloud is the deployment model most widely used as well as that which carries the clearest benefits of cloud computer versus traditional IT. Rather than invest in building, operating, and maintaining proprietary data centers in order to deliver digital ID services, a government can contract the provision of computing resources on an as needed basis, governed by contracts and service level agreements with a CSP tightly specifying performance standards and the rights and responsibilities of all parties.

Digital ID systems rely on persistent storage of data—for example user identifiers—as well as the processing and network management capabilities to respond to authentication requests. These capabilities can run on cloud services as effectively, if not better, than on any private or government managed data center. The provision of storage and compute infrastructure is software-neutral and can accommodate multiple different solutions a government may wish to deploy.

In addition, cloud providers can provision and deprovision resources elastically as customers need them. In contrast to dedicated and on premises hardware which lie unutilized for significant amounts of time, this allows for efficient and agile management. This capability is particularly beneficial for digital identity, where usage demands may shift significantly, spiking at certain times but lying dormant at others. Provisioning and the economies of scale that come with it is most elastic in cloud services, rather than on premises, which operates on a finite pool of dedicated computing resources which may sit unutilized for stretches of time. The flexibility of the cloud enables it to be a platform for new innovations. Rather than be locked into procured in-house capabilities, governments leveraging cloud for digital ID can more quickly develop and deploy it in government services. This has been especially important during the COVID-19 pandemic, where cloud has enabled resilient public services, from continued and newly urgent delivery of social transfers to new virtual services like online education. Further, cloud computing constitutes a significant and growing segment of private sector IT spend and a dynamic sector for innovation. Following suit allows the government to adopt new innovations to improve their digital ID systems more quickly as well as attract and retain quality talent.

Contents

› **Introduction**

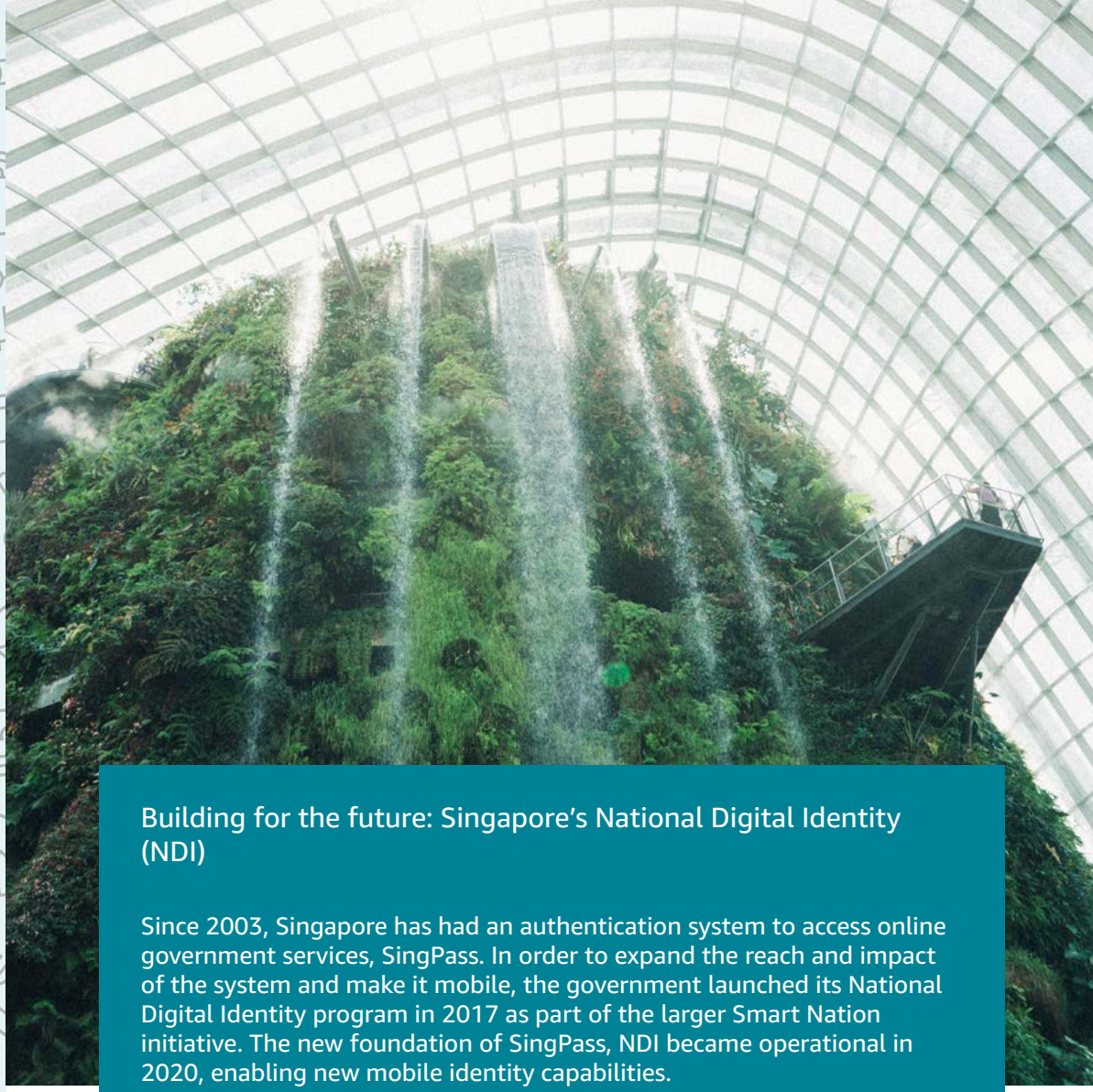
› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**



Building for the future: Singapore's National Digital Identity (NDI)

Since 2003, Singapore has had an authentication system to access online government services, SingPass. In order to expand the reach and impact of the system and make it mobile, the government launched its National Digital Identity program in 2017 as part of the larger Smart Nation initiative. The new foundation of SingPass, NDI became operational in 2020, enabling new mobile identity capabilities.

NDI provides a common platform for government services as well as secure transactions with the private sector. It was designed from the ground up to be in the cloud, using a multi-cloud architecture for maximum resilience. This enabled the construction of a more flexible and scalable system that could serve as the basis of many public and private services not specifically planned at the inception. The government of Singapore created a developer platform and sandbox environment that enables external partners to build and integrate e-services with NDI in new ways.

This has allowed the creation of a set of APIs open to government and the private sector such as MyInfo, Login, Verify, Authorize, Sign, and Face. MyInfo, for example, is a digital vault of personal information that individuals can choose to disclose to government and private entities for services such as opening a bank account or accessing financial services (Smart Nation Singapore 2021; Computer Weekly 2018).
Crucially, this flexible system facilitated rapid deployment of new e-services during the COVID-19 pandemic. Various new services have been built on top of NDI, including the national contract tracing app TraceTogether, the SafeEntry QR code-based entry management, and the system of health passports HealthCert, which allow seamless integration from issuance of a certificate by a vaccination clinic through generation of a QR code to verify vaccination status when needed (Singapore Government Developer Portal 2021).

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Myths and mindsets hamper effective digital ID

The design decisions of digital ID systems are critical and strategic in their ability to ensure that a country may have access to benefits quickly and more efficiently. Unfortunately, certain common misconceptions around digital identity—particularly when implemented using cloud computing—can lead to decisions which frustrate strategic goals. Misconceived ideas lead countries to favor approaches that result in higher expense and less flexible and robust systems. Policy makers should challenge these ideas and keep an open mind regarding the technical decisions underpinning successful systems.

Myth 1: Digital ID systems should require localization for security reasons

Because of the pivotal role they can play in enabling transactions between individuals, the government, and the private sector, as well as privacy concerns to safeguard personal data, governments rightly keep a strong focus on ensuring that digital ID systems are well secured. However, policymakers often see the best way to pursue this to mean keeping data tightly localized in one or a small number of systems, whether controlled by the government or a private contractor. Direct control over the data and its storage location is frequently perceived as a critical factor. This results in conditions on where private sector actors keep data, called data residency, when they provide a public digital ID system.

The reality is that location is no guarantee of security, and this approach hampers the ability to grow and develop a digital ID system to its fullest. In fact, data residency rules are counterproductive to ensuring that data is kept securely. Storage in a single location, especially when managed on premises, may provide a single point of failure as well as an enticing target for malicious actors. Should they be successful—for example, by finding a piece of unpatched software or configuration error—any breaches may then inflict maximum harm. Even though providing the appearance of control through proximity or physical access, this approach in fact leaves data more vulnerable. Ensuring true security depends on multiple factors that are agnostic regarding location, including encryption protocols, system configuration, software patching protocols, physical security measures, and access management.

Localization also entails added expense. Most benefits of digital identity derive from systems that are deployed as widely as possible. This means serving all of the population and enabling sufficient flexibility for public and private actors to develop new capabilities on top of the platform that digital identity provides. Matching the scale and variability of demand this entails requires a robust and elastic system that is simply not possible or too expensive for most government entities to build and run efficiently. A cloud-based architecture, including leveraging the capabilities of hyperscale cloud providers, would allow deployment of these systems at scale.

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Hyperscale cloud providers can, in fact, be safer than local infrastructure. Large commercial providers can leverage considerable resources and global expertise in order to implement and maintain the highest quality protections available, such as:

- Advanced physical safeguards and protocols to control access to hardware
- High quality encryption
- Real-time monitoring for security incidents
- Detailed audit logs
- Hardware-level encryption
- Highly verified supply chains, better guarding against the introduction of unknown vulnerabilities

Hyperscale cloud providers also offer advantages in terms of availability and resilience that on-premises solutions lack. When stored across different segregated geographic regions and/or with duplicate backups, cloud providers can provide a greater level of certainty and resilience to disruption than a single data center can—whatever its location.

Bound by customer contracts and strongly incentivized to maintain a reputation for reliability, providers are highly skilled at implementing security, including upgrading technologies, and implementing updates to patch newly discovered vulnerabilities. Ultimately, these security capabilities, which large professional providers are best situated to provide, are the critical factors that can ensure a trusted and secure digital ID system, not location.

Myth 2: Digital ID systems lead to privacy risks

Digital ID systems can play an important part of individuals' lives, from accessing critical services to conducting sensitive transactions. As consumers become more aware of online threats and breaches of their personal data, a digital ID system can look like another source of vulnerability. Especially in countries with a history of controversy over surveillance. And even in those countries where government access to citizen information is regarded as the norm, they can also look like an opportunity for authorities to access personal data in a manner that individuals may not be comfortable with. These concerns may be especially acute when data is stored in the cloud. The idea of data being held by a private party or stored in another jurisdiction subject to different laws can raise concerns.

The reality is that physical systems and on-premises storage of data are in practice less secure and private, whereas digital and cloud-based systems—especially when managed by professional cloud service providers, many of which are internationally certified to recognized privacy benchmarks—can offer important privacy-enhancing capabilities.

In practice, governments managing digital ID systems have less access to data than may be sometimes feared. Even in highly centralized systems, detailed data on individuals is not necessarily what is concentrated at the center of the system. Only a minimal amount of data is required to perform the core authentication function, such as basic identifiers and biometric templates. Transaction information or profiles of the individual are not required and can be discarded or held at the point of the individual interaction.

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

Minimizing data used: India's Aadhaar

The implementation of the Aadhaar system and the integration of additional services has led to cybersecurity challenges. However, initial fears of the system creating a privacy-violating surveillance mechanism have not come to pass.

The Aadhaar system is based on a centralized database of biometric signatures and identifiers. However, it does not hold a significant amount of information. The core Aadhaar system only stores and processes five pieces of information: name; gender; date of birth; address; biometric signature (not the full data used to generate this template); and, in some cases, name of spouse or guardian. Actual biometric information, which cannot be reconstructed from the template, is archived and generally inaccessible. These pieces of information are split up and stored in different locations and only accessed and assembled as needed in order to execute authentication. This helps to ensure that even in cases of misuse or breach, only limited data is accessible.

Privacy risks exist with legacy paper systems as well, frequently to an even greater degree. Physical records may need to be stored in multiple locations when authentication is carried out, cannot be encrypted, and can only be protected with physical safeguards. This means that any party improperly accessing physical files or intercepting correspondence in paper systems can access critical information.

By contrast, digital systems do not necessarily leave behind retained records or copies once authentication has been carried out. Critical information throughout the process can (and should) be encrypted both at rest and in transit and information automatically destroyed when no longer needed.
Large cloud providers can provide further benefits. These parties have robust contractual and technical measures in place to prevent unauthorized access. In addition to the security advantages discussed above to prevent improper access and safeguard the integrity and availability of data, cloud providers implement a shared security framework which can empower the customer with control over core aspects of security. This means cloud providers often do not have access to customer data or directly manage its level of security apart from physical security. These and other clear safeguards are built into contracts and service level agreements to make sure data in the cloud is maintained at the level of security and confidentiality the client dictates.

For the most sophisticated providers, these are implemented with stringent protocols for staff, strategically designed network architectures and infrastructure locations, as well as technical safeguards down to the hardware level that make it nearly impossible for outside parties to access data. The use of cloud regions by large providers, for example, make it possible for a party contracting cloud services to decide to only store their data in certain trusted geographies.

Measures to shield data can even sometimes protect it from access requests by foreign governments, as technical and organizational measures such as encryption can make it technically impossible for cloud providers to respond to disclosure requests. Commercially, these providers have strong incentives to respect their commitments and client expectations. A track record of failures to honor their contractual commitments is a sure route to losing customers in the competitive global markets for cloud computing.

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

Myth 3: Digital ID is expensive and only attainable for advanced economies

Implementing a national digital ID system requires investment in technology resources as well as reengineering of processes across government departments who intend to use the system. This leads to the perception that digital identity is expensive and therefore only attainable for advanced economies.
In fact, the infrastructure and technology for digital identity are now widely available and cheaper every day. Today, approximately 159 countries around the world, most of which are developing countries, implement some form of digital ID (World Bank ID4D Dataset 2018). Some of the biggest successes in digital identity come from developing countries, such as India, which has implemented the largest such system in the world.

In some areas of technology adoption, development of more advanced technology can create new digital divides, as wealthy countries adopt advancements before developing countries. For digital identity, the current state of technology suggests the opposite. The growth of cloud computing is driving down the costs of high-quality storage, processing, and software, transforming it into a universally accessible utility.

Similarly, increasingly pervasive and affordable mobile technology creates opportunities for verifying digital identity simply with mass consumer devices rather than dedicated hardware. These capabilities enable more rapid adoption of new advancements such as in biometrics and speed up the process of quickly integrating new services and innovations. New open-source platforms like the Modular Open Source Identity Platform (MOSIP) create a freely available and software agnostic architecture countries can use as a template for their systems. Use of cloud services is further reducing the cost of implementing digital identity. The global growth of cloud computing and the economies of scale attained by large providers with global networks is transforming computing into something akin to a utility—a reliable, standardized service available anywhere with an internet connection. This makes access to the high-quality computing resources necessary to support digital identity available and affordable to many governments, even those without significant means.

As a result, developing countries have an opportunity to leverage these advantages and leapfrog ahead. By starting with the latest and most flexible technology, they can quickly implement high quality digital ID systems that are fit to purpose and adaptable.

Keeping an open mind

As they weigh the different technical options before them in developing digital identity, policy makers should keep an open mind and holistically evaluate the costs, benefits, and tradeoffs of the technologies that best support their priorities. Overcoming the above misconceptions is crucial, as they in many cases obstruct consideration and adoption of the most effective cloud-based approaches to digital identity.

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Policymakers should keep a full view of the possible benefits of all approaches, not just potential risks. Myths, including around cloud computing, can lead them to pursue approaches that provide the appearance of prudence and control at the expense of inferior protections, higher costs, and less robust capabilities.
On the contrary, implementation of a digital ID system through cloud computing helps practitioners focus on and develop the best methods to overcome the most relevant challenges, namely how to:

- Enable future system growth, expansion, and innovation using digital ID as a base
- Minimize the data collected and utilized in order to build trust
- Design effective safeguards to keep sensitive data protected, not limited to location

Cloud emerges as a clear best practice and a powerful advantage for any national digital ID system. However, the decision to use cloud is just one component of effective design and implementation. What are the other key considerations to ensure an effective digital ID system? The following chapter will develop this line of inquiry further, to examine some additional best practices which enable successful implementation of digital ID systems from key design considerations to steps that ensure smooth roll out and wide adoption.

Contents

› **Introduction**

› Chapter 1:
The opportunity of digital identity

› Chapter 2:
Digital ID structures

› Chapter 3:
Designing an effective digital ID system

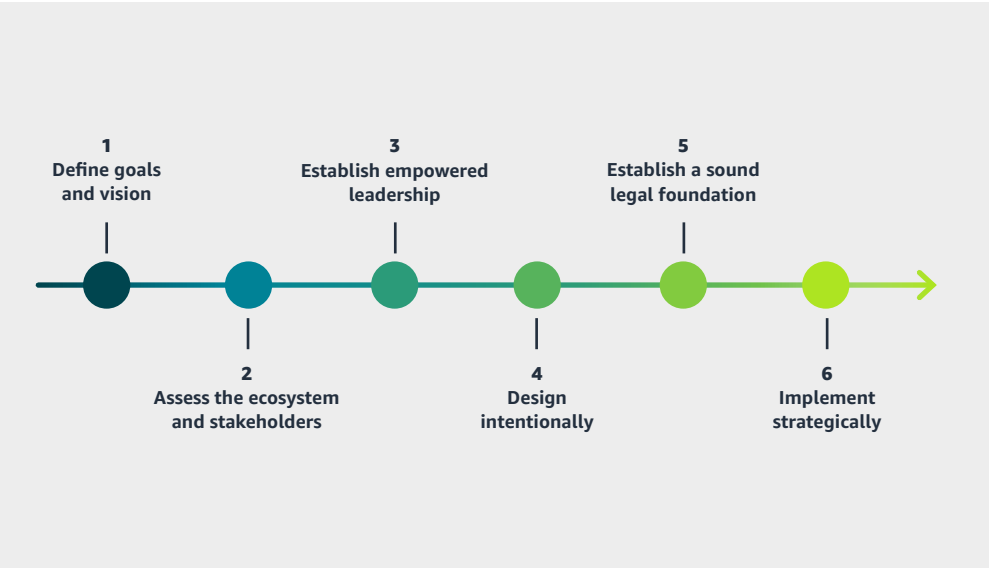
› Chapter 4:
Lessons learned and best practices

› **Bibliography**

Chapter 4:
Lessons learned and best practices

Whether building a system from scratch or updating and expanding existing parts of the identity ecosystem, implementing a digital ID system is complex. Achieving a successful digital ID system which delivers benefits for the population is about much more than writing code and application software. Rather than applying a single technology template, it should be thought of more as a process to re-engineer systems in pursuit of social goals, with many steps between inception and a functioning system.

To carry an initiative forward, countries need not just technical features for success, but the right process and mindset to ensure a smooth roll out that provides advantages for all stakeholders.



1. Define goals and vision

From the start, those developing a digital ID system should have a very clear mission and vision. A clear vision of the path a country it setting out on and the desired end goals makes it easier to plan the way forward and navigate complications as they arise. This vision should align across core stakeholders. For example, a government agency that fully understands and supports from the beginning that a new foundational system will replace their existing functional system is less likely to create challenges mid-way through a project when they come to understand its full implications for how they manage public services.

Effective digital ID systems put people at the center, and design must start with people. Individual citizens understand the ground realities of public services requiring identity authentication and can help define goals that will provide the greatest good. Actively seeking and centering their views in conversations around digital ID, and system design can focus planning in the most productive areas as well as dispel concerns early—for example, around privacy, security, and data use. As part of coalescing a cohesive and achievable vision, consultation with parties directly involved in managing and deploying uses cases is crucial—especially public and private sector entities who may implement major use cases as well as the private parties with technical expertise. This helps to ensure a vision is achievable and considers the technical role of different stakeholders.

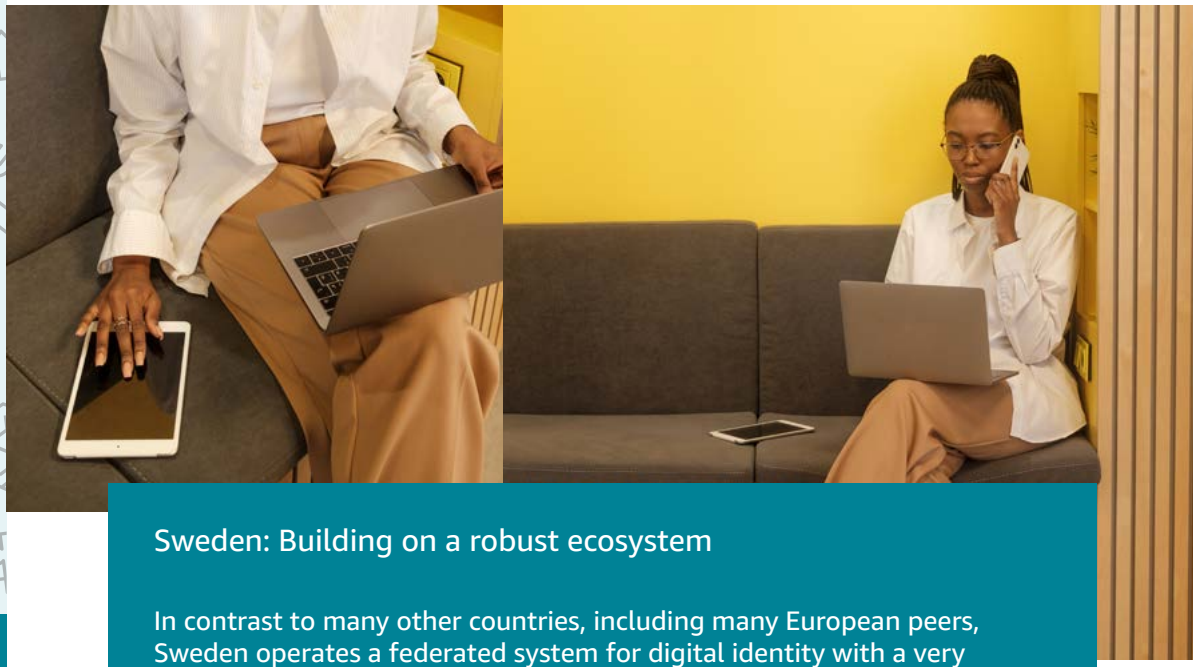
Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

2. Assess the ecosystem and stakeholders

Countries begin the process of adopting digital ID with different government and private entities already playing some role in establishing, verifying, and utilizing identity, digital or not. Depending on the level of economic and technological development a country starts with, citizens may already possess various digital and non-digital identities issued by public and private parties that they use for functional purposes, including banking, public records, online transactions, or social benefits. Which IDs already exist and their technical features are important to assess, as they may provide building blocks for a more comprehensive system, illuminate quicker paths to success, or indicate areas where stakeholders may resist changing current systems.

Countries are also embedded in local, regional, and global ecosystems of technology providers, implementers, and users who may be able to play a valuable role. Assessing the availability of capacity for building and implementing a digital ID system is important for informing technical and programmatic plans. Identifying gaps in local capacity that can be filled by international providers are also important for taking make or buy procurement decisions of different elements. If there are robust local players, seeking to identify local champions in the technology ecosystem can also yield an indispensable ally to help bring the private sector or other stakeholders along with changes.



Sweden: Building on a robust ecosystem

In contrast to many other countries, including many European peers, Sweden operates a federated system for digital identity with a very strong role for the private sector. As electronic services and the need for online authentication grew in the late 1990s and early 2000s, Sweden approached the issue in view of its long history of private sector-issued identification issued by institutions such as banks and post offices (Grönlund 2010). Instead of constructing a new system from scratch, it decided to recognize, promote, and coordinate the use of multiple private digital IDs checked against national population register personal identity numbers, all of which would be accepted by the government.

The most widespread digital ID in Sweden is the private BankID provided by an 11-bank consortium as well as one issued by telecom operator Telia. Leveraging a market-driven federated model has achieved a high but not universal penetration rate, with 91.9 percent of Swedish citizens holding a BankID by 2017, which was accepted by over 200 government agencies (OECD 2018). To achieve even higher rates, especially for marginal populations and migrants, the government is exploring an additional complementary public digital ID.

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

3. Establish empowered leadership

Taking a digital identity system from inception to launch is a long and complex process involving many stakeholders. Government services and the technology underpinning them often work within silos. Cooperation and participation in a shared platform may not always come naturally. To overcome barriers along the way and keep a program moving forward, an initiative needs appropriately high-level leadership who can take ownership and drive it forward. Explicit support from senior members of the government is indispensable.

Digital ID programs also need to have access to appropriate technical expertise. The best strategic decisions can be made when leadership is well advised regarding all aspects of the project, political and technical, and understand the full implications of all options. Well-staffed and informed teams can confidently make decisions and deftly engage with all phases of the process, from consultation through design, development, and implementation. In many cases, this may mean close consultation or even formalized engagement with key private sector actors with experience in these areas.

Singapore: Pushing modernization with top level support

Though it has a history of robust government IT systems and e-services, as well as a long standing non-digital foundational ID, Singapore has only within the last few years moved to adopt a comprehensive digital ID system. The government recently launched the National Digital Identity (NDI) Programme to build on other existing widespread functional digital IDs like SingPass. Led by GovTech, the dedicated agency for government technology transformation and e-services, NDI is embedded in the Smart Nation initiative, a marquee effort of the government with the highest-level support. NDI in particular is promoted as a key part of Smart Nation, and has been referred to by Prime Minister Lee Hsien Loong as the "cornerstone" of the initiative. This priority gives GovTech a strong mandate to move forward, gather stakeholders together, and overcome barriers. Senior Director of the NDI program Quek Sin Kwok has stated that this support is critical, and that he feels "fortunate that I have very strong support from political holders. Everyone is in sync that this is something we have to do," (CIO 2019).

4. Design intentionally

After forging a common vision, a set of goals, and establishing leadership, program leaders need to design the technical architecture of their digital ID system. Even though different approaches all have their respective advantages as well as costs in the near term, these early decisions also have enormous downstream implications for how the system will grow and adapt well after its launch and initial use cases are achieved. Some choices will support the ability of government entities and private sector partners to quickly and securely innovate, experiment, and improve services leveraging digital ID; other approaches can integrate systemic flaws or make it challenging to expand. It is therefore crucial to bake in design features, which get the fundamentals right without constraining future growth and innovation.

Taking into account the desired end-goals, the sophistication of the existing ecosystem and other known constraints, policy-makers must make several fundamental design selections, including: a foundational or functional model; a centralized, federated, decentralized, or open market architecture; as well as an instrumental or infrastructural deployment. They also must decide which data attributes the system will process, how they will be gathered, and how they will

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

be managed, including the biometric characteristics that may be well suited for use in the system, which in most cases requires external vendors. This invites consideration of issues including data standardization, interoperability, and minimization, important aspects not just of usability of the system but of user trust. Taking a privacy-by-design orientation to designing data systems will help to build in trust from the start.

These decisions are highly consequential for the long-term uptake and sustainability of digital ID systems. Policy makers should have a strong bias towards foundational and infrastructural approaches, as well as the use of the cloud and open-source technology. These provide the best platform to reach the widest number of citizens as quickly as possible and support both public and private sector innovation in the long term. Inherently open, scalable, and resilient, these approaches let policymakers set the stage for future successes by enabling a wide swath of organizations to build new services and capabilities not yet envisioned. This creates a real opportunity to build once and then let others take advantage of the platform the government creates rather than duplicate systems for each service.

Design should also look forward to and seek to make decisions that will facilitate faster uptake and deployment. Technical design should look to leverage existing ecosystem capabilities to the greatest extent feasible and consistent with core performance needs of the system. Consideration should be given to the needs of potential high impact uses cases, skills and capabilities of responsible staff, as well as ease of individual registration and use. Additionally, proprietary technologies and specialized hardware can be a serious bottleneck that hamper rapid deployment and inclusion and should be avoided.

5. Establish a sound legal foundation

The legal foundations for digital ID are crucial to putting it on a firm and sustainable footing, and governments should take care to assess and revise the laws that can either support or hamper the long-term viability of a digital ID system.

Digital identity cannot exist without a legal purpose. The provisions giving purpose to digital ID and specifying its status as acceptable identity verification must be embedded in relevant legislation—for example, laws and regulations governing the verification of legal identity for property transactions or tax payment. Foundational systems in particular are often embedded in systems such as birth or population registries which generally provide unique personal identifiers. Basic elements of digital government and digital transactions, such as legal recognition of eSignatures, are likewise prerequisites to ensure viable use cases.

Considering the legal foundations underpinning digital ID also presents an important opportunity to build trust from the start. Public trust can be fragile, and countries that don't invest in ensuring the public understands how the system works, how it will be governed, and rights and protections vis-à-vis personal data have sometimes met resistance. For example, Aadhaar roll out in India has received push back from watchdogs concerned about government surveillance and data security. Getting the right pieces in place to foster this trust is especially crucial in countries with histories of sensitivities regarding privacy and government access. As such, adoption or revision to legislation on personal data protection to establish protections in line with global best practices may be an important element for some jurisdictions to have in place prior to implementing digital ID, as would sufficient measures to ensure data security. Private sector involvement and intermediaries can be an important route to build trust as well. Involvement of the financial services sector can be particularly powerful due to the existing trust between users and banks, as well as the frequency with which users use financial services tools.

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

Kenya: Supreme Court challenge disrupts implementation

In 2020, the government of Kenya operationalized the National Integrated Identity Management System (NIIMS), a foundational digital ID system that would link together various national identity and vital statistic data sources to create a single biometric database. The program was initiated by Executive Order in 2018, prior to implementation of the Data Protection Act in 2020. Various civil society organizations have expressed concerns regarding the privacy and security controls built into the system, ultimately culminating in a judicial case that reached the Kenyan Supreme Court. In October 2021, the Supreme Court ruled against the government, in particular the issuance of the biometric Huduma cards under the program, finding that the protections of the Data Protection Act must be applied retroactively to the roll out of the program. Stating that the government had "put the cart before the horse," the court ordered the government to conduct a data protection impact assessment of the identity card program and develop further regulations. It also barred the collection of any DNA or geo-location data. Further court cases are pending, contributing to the delay and uncertainty surrounding the initiative and undermining its social value (Open Society Justice Initiative, 2021).

6. Implement strategically

After getting the first elements into place—a clear vision, coordination with stakeholders, strong leadership, coherent technical design, and sound legal foundations—a digital ID program must be implemented and rolled out to the population. Possibly the most delicate part of the journey, poor implementation can hold back use, undermine trust, and lead to delays. This requires a careful plan and a strategic approach.

Implementing a large cross government IT-enabled project is a political challenge as much as a technical one. Coordinating with various public sector entities requires a keen attention to effective messaging, relationship management, and understanding of the political economy stakeholders face. Starting right requires understanding what they already think and perceive about digital ID and what their needs are. On this basis, teams can develop the best ways to communicate what digital ID will mean to a range of stakeholders. Fostering the understanding with the right stories, messages, and prototypes that a digital ID project is positive and additive, rather than subtractive or intended to replace current systems can ease the process of bringing political and bureaucratic stakeholders along. Getting them excited about what the vision can do for them rather than defensive about perceived criticism of their systems is a key mindset. Finding ways to secure quick wins that show concrete value, such as through demonstration projects, can also get buy in from stakeholders.

Similarly, having a single, high-impact use case can be a powerful tool to drive a project forward and show that it can work. Starting first with implementing digital ID to solve a long-standing problem or improve citizen experience of a single service on a large scale builds popular and political support for continuing to push forward wider implementation. This gets users interacting with the system and seeing and understanding its benefits.

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Partnership with key stakeholders can also be indispensable to implementing specific use cases and facilitating uptake. Touchpoints between citizens and the government can become a key point to promote or require the use of a new digital ID. Private sector businesses or civil society groups come with strong connections to the community and can be powerful interlocutors to build trust and advocate for uptake and use. Securing their support or deputizing them to enroll citizens in the system can also be a powerful tool to quickly reach a large proportion of the population.

India: The analogue underpinnings of digital success

India is widely hailed as one of the most impactful deployments of foundational digital ID around the world, where over 1 billion people have rapidly been enrolled in the Aadhaar system. Successful roll out and uptake of Aadhaar relied on a huge ecosystem—much of which has little to do with technology. To achieve rapid uptake, support and active assistance was needed from a wide array of partners, including different actors in the private sector and various national and state level public stakeholders. The system relies on having multiple registrars to enroll people in the program – in principle, any organization interfacing with the public can serve as a registrar, including banks, state government food ration shops, insurance companies, and social service organizations.

In addition to leveraging banks and other private groups to rapidly enroll people, the government linked the use of Aadhaar to the distribution of certain public benefits, including cash transfers for the purchase of cooking fuel by those with low incomes. The largest direct benefit transfer system in the world, the scheme served 177 million persons. This facilitated rapid deployment as well as improvements in the delivery of benefits (Mittal, Mukherjee, and Gelb).

In combination, these two factors became powerful levers to get millions of persons enrolled in the system, demonstrate how it could succeed, and facilitate its wider use for other social benefit schemes and government services.

Finally, due attention must be given to the readiness of the public to understand and utilize their new digital ID. In countries without high Internet penetration or familiarity with digital services, additional measures to educate and increase digital literacy may be needed. Empowering them with a baseline to conceptualize what it means and understand how to use it enables citizens to take full advantage of what a digital ID can offer and helps private sector businesses to develop and offer services. Careful attention to these factors can also help to identify potential pitfalls where there may be barriers to adoption or preferences for analogue interactives.

Contents

› **Introduction**

› Chapter 1: **The opportunity of digital identity**

› Chapter 2: **Digital ID structures**

› Chapter 3: **Designing an effective digital ID system**

› Chapter 4: **Lessons learned and best practices**

› **Bibliography**

Lessons Learned

This report has laid out considerations and examined the experiences of diverse countries with digital identity—all aimed at articulating what constitutes a well-designed digital ID system. Even though there is no single model that answers this question for every country, a survey of the landscape reveals that there are core processes, considerations, and technical decisions that will help countries maximize the benefits of digital identity and transform public services.
At the end of their digital identity journey, despite differing national goals and priorities, countries aim to have a digital ID system that is: widely adopted and inclusive; cost effective; trustworthy; enabling of public service improvement and innovation; supportive of economic growth; and flexible for future change, expansion, and experimentation.

To achieve these ends as quickly as possible and to develop systems that are sustainable in the long run, some critical success factors emerge from the experiences of countries which have implemented digital ID:

- Focus on the **needs and experiences of people** to design the system that will be accepted and used willingly
- Systems **open to the private sector** maximize positive impact for innovation and economic growth, especially when implemented via API building blocks
- Focus on **accelerating the transformation of public services** can help governments to better respond to citizen's needs
- Adoption of **carefully thought through supporting legislation and regulation** ensures long term legal stability and fosters social trust
- **Foundational and infrastructural** approaches create platforms that can adapt and be built upon by others
- **Open source**-based systems help ensure interoperability and cost-effectiveness
- **Cloud**-based approaches provide maximum scalability, agility, security, and resilience in response to changing needs

Through effective deployment of digital ID, countries around the world can achieve real impacts for their citizens. As countries rise to the identity challenge, we can unlock exciting opportunities to help those most in need of legal identity, improve the quality and availability of public services, and promote innovation and a growing digital economy that benefits all.

Contents

› **Introduction**

› Chapter 1:
The opportunity of digital identity

› Chapter 2:
Digital ID structures

› Chapter 3:
Designing an effective digital ID system

› Chapter 4:
Lessons learned and best practices

› **Bibliography**

Bibliography

Abell, Thomas, Arndt Husar, and May-Ann Lim. 2021. Cloud Computing as a Key Enabler for Digital Government across Asia and the Pacific. Asian Development Bank. ***https://www.adb.org/publications/cloud-computing-digital-government-asia-pacific.***

Access Now. 2018. 'National Digital Identity Programmes: What's Next?'

Bayuo, Blaise, and Sophie Tholstrup. 2021. 'The Fundamentals of Tech Transformation: Identity in a Digital Age.' Tony Blair Institute for Global Change. ***https://institute.global/policy/fundamentals-tech-transformation-identity-digital-age.***

Clark, Julia Michal. 2018. 'Public Sector Savings and Revenue from Identification Systems : Opportunities and Constraints.' Text/HTML. Washington, D.C: World Bank Group. ***https://documents.worldbank.org/en/publication/documents-reports/documentdetail/745871522848339938/Public-Sector-Savings-and-Revenue-from-Identification-Systems-Opportunities-and-Constraints***.

Clark, Julia Michal, Anneke Elizabeth Schmider, Luda Bujoreanu, Jonathan Marskell, and Ana Milena Aguilar Rivera. 2018. 'The Role of Digital Identification for Healthcare: The Emerging Use Cases.' Text/HTML. Washington, D.C: World Bank Group. ***https://documents.worldbank.org/en/publication/documents-reports/documentdetail.***

Computer Weekly. 2018. 'Singapore Extends Reach of Digital ID System with Cloud.' ComputerWeekly.Com, 10 October 2018. ***https://www.computerweekly.com/news/252450331/Singapore-extends-reach-of-digital-ID-system-with-cloud.***

Crowe, David. 2021. 'MyGov to Get $200m Upgrade in Digital Services Overhaul.' The Sydney Morning Herald, 5 May 2021, sec. Federal. ***https://www.smh.com.au/politics/federal/mygov-to-get-200m-upgrade-in-digital-services-overhaul-20210505-p57p7o.html.***

Desai, Vyjayanti, Anna Diofasi, and Jing Liu. 2018. 'The Global Identification Challenge: Who Are the 1 Billion People without Proof of Identity?' World Bank Blog (blog). 25 April 2018. ***https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity.***

Dighe, Amy, Lorenzo Cattarino, Gina Cuomo-Dannenburg, Janetta Skarp, Natsuko Imai, Sangeeta Bhatia, Katy A. M. Gaythorpe, et al. 2020. 'Response to COVID-19 in South Korea and Implications for Lifting Stringent Interventions.' BMC Medicine 18 (1): 321. ***https://doi.org/10.1186/s12916-020-01791-8.***

e-Estonia. 2017. 'A Digital Success Story: The Cornerstone of e-Estonia Celebrates Its Jubilee.' 31 January 2017. ***https://e-estonia.com/a-digital-success-story-the-cornerstone-of-e-estonia-celebrates-its-jubilee/.***

d-Estonia. 2018. 'What We Learned from the EID Card Security Risk?' E-Estonia (blog). 14 May 2018. ***https://e-estonia.com/card-security-risk/.***

G20. 2021. 'Declaration of G20 Digital Ministers: Leveraging Digitalisation for a Resilient, Strong, Sustainable and Inclusive Recovery.' ***https://www.g20.org/wp-content/uploads/2021/08/DECLARATION-OF-G20-DIGITAL-MINISTERS-2021_FINAL.pdf.***

GSMA. 2018. 'Using Mobile Technology to Provide Functional Identities.' GSMA Blog (blog). 22 January 2018. ***https://www.gsma.com/mobilefordevelopment/blog-2/using-mobile-technology-provide-functional-identities/.***

Iyer, Neema. 2021. 'Uganda: Are Digital IDs a Tool for Inclusion or Exclusion?' Research ICT Africa (blog). 23 June 2021. ***https://researchictafrica.net/2021/06/23/uganda-are-digital-ids-a-tool-for-inclusion-or-exclusion/.***

Joon Song, Hee, Minah Kang, Churin Kim, and Yeonsoo Kim. 2016. 'Korea: An Integrated System of Civil Registration and Vital Statistics.' Text/HTML. Washington, D.C: World Bank Group. ***https://documents.worldbank.org/en/publication/documents-reports/documentdetail.***

Kharas, Homi. 2020. 'The Impact of COVID-19 on Global Extreme Poverty.' Washington, D.C: Brookings Institution. ***https://www.brookings.edu/blog/future-development/2020/10/21/the-impact-of-covid-19-on-global-extreme-poverty/.***

Krishna, Geetanjali. 2018. 'Fixing Aadhaar Bugs: Putting a Finger on the Biometric Problem.' Business Standard India, 16 January 2018. ***https://www.business-standard.com/article/economy-policy/fixing-bugs-of-aadhaar-putting-a-finger-on-the-biometric-problem-118011501030_1.html.***

Lowmaster, Kaelyn. 2018. 'Private Sector Economic Impacts from Identification Systems.' Text/HTML. Washington, D.C: World Bank Group. ***https://documents.worldbank.org/en/publication/documents-reports/documentdetail/219201522848336907/Private-Sector-Economic-Impacts-from-Identification-Systems.***

McKinsey Global Institute. 2019. 'Digital Identification: A Key to Inclusive Growth.' ***https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth#.***

Mell, Peter, and Tim Grance. 2011. 'The NIST Definition of Cloud Computing.' Gaithersburg, MD: United States National Institute of Standards and Technology (NIST). ***https://csrc.nist.gov/publications/detail/sp/800-145/final.***

Contents

- **Introduction**
- Chapter 1: **The opportunity of digital identity**
- Chapter 2: **Digital ID structures**
- Chapter 3: **Designing an effective digital ID system**
- Chapter 4: **Lessons learned and best practices**
- **Bibliography**

Contents

› **Introduction**

› Chapter 1:
The opportunity of digital identity

› Chapter 2:
Digital ID structures

› Chapter 3:
Designing an effective digital ID system

› Chapter 4:
Lessons learned and best practices

› **Bibliography**

Mittal, Niraj, Anit Mukherjee, and Alan Gelb. 2017. 'Fuel Subsidy Reform in Developing Countries: Direct Benefit Transfer of LPH Cooking Gas Subsidy in India.' Center for Global Development Policy Paper 114. December 2017. ***https://www.cgdev.org/sites/default/files/fuel-subsidy-reform-developing-countries-india.pdf***

Muralidharan, Karthik, Paul Niehaus, and Sandip Sukhtankar. 2020. 'Identity Verification Standards in Welfare Programs: Experimental Evidence from India.' w26744. Cambridge, MA: National Bureau of Economic Research. ***https://doi.org/10.3386/w26744.***

Omidyar Network India and Boston Consulting Group. 'MOSIP: Open Digital Ecosystem (ODE) Case Study.' ***https://opendigitalecosystems.net/pdf/04_MOSIP-Case-Study_vF.pdf***

Open Society Justice Initiative. 2021. 'New Kenya High Court Judgment Sets Important Precedent for Digital ID Privacy Protections and Processes.' 15 October 2021. ***https://www.justiceinitiative.org/newsroom/new-kenya-high-court-judgment-sets-important-precedent-for-digital-id-privacy-protections-and-processes***

Privacy International. 2021. 'Exclusion by Design: How National ID Systems Make Social Protection Inaccessible to Vulnerable Populations.' Privacy International (blog). 29 March 2021. ***http://privacyinternational.org/es/node/4472.***

Reuben, William, and Robert J. Palacios. 2018. 'ID4D Country Diagnostic: Peru.' Text/HTML. Washington, D.C.: World Bank Group. ***https://documents.worldbank.org/en/publication/documents-reports/documentdetail/245571518449918214/ID4D-Country-Diagnostic-Peru.***

Saarinen, Juha. 2020. 'Researchers Say Not to Use MyGovID until Login Flaw Is Fixed.' ITnews, 21 October 2020. ***https://www.itnews.com.au/news/researchers-say-not-to-use-mygovid-until-login-flaw-is-fixed-553601.***

Singapore Government Developer Portal. 2021. 'Digital Solutions for a 21st Century Pandemic – COVID-19 Technologies.' Singapore Government Developer Portal. 16 September 2021. ***https://www.developer.tech.gov.sg/technologies/digital-solutions-to-address-covid-19/overview.***

Smart Nation Singapore. 2021. 'National Digital Identity (NDI).' Default. 2021. ***https://www.smartnation.gov.sg/what-is-smart-nation/initiatives.***

Solomon, Brett. 2018. 'Digital IDs Are More Dangerous Than You Think.' Wired, 28 September 2018. ***https://www.wired.com/story/digital-ids-are-more-dangerous-than-you-think/.***

The Economic Times. 2018. 'Aadhaar-Enabled DBT Savings Estimated over Rs 90,000 Crore.' The Economic Times, 11 July 2018. ***https://economictimes.indiatimes.com/news/economy/finance/aadhaar-enabled-dbt-savings-estimated-over-rs-90000-crore/articleshow/64949101.cms.***

UNESCO, and EQUALS Skills Coalition. 2019. 'I'd Blush If I Could: Closing Gender Divides in Digital Skills through Education.' ***https://unesdoc.unesco.org/ark:/48223/pf0000367416.page=1.***

Unique Identification Authority of India. 2021. 'Aadhaar Dashboard.' 2021. ***https://uidai.gov.in/aadhaar_dashboard/.***

United Nations General Assembly. 1948. Universal Declaration of Human Rights. ***https://www.un.org/en/about-us/universal-declaration-of-human-rights.***

United Nations General Assembly. 1966. International Covenant on Civil and Political Rights (ICCPR). ***https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.***

United Nations Department of Economic and Social Affairs, Statistics Division. United Nations Legal Identity Agenda. ***https://unstats.un.org/legal-identity-agenda/***

USAID. 2017. 'Identity in a Digital Age: Infrastructure for Inclusive Development.' ***https://www.usaid.gov/digital-development/digital-id/report.***

World Bank. 2016. 'Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation.' World Bank Group. ***https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf.***

World Bank. 2017. 'The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution.' Washington, D.C: World Bank Group. ***https://openknowledge.worldbank.org/bitstream/handle/10986/29510/211259ov.pdf.***

World Bank. 2019a. 'ID4D Practitioner's Guide.' Washington, D.C: World Bank Group. ***https://id4d.worldbank.org/guide.***

World Bank. 2019b. 'Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable.' Washington, D.C: World Bank Group. ***https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable.***

World Bank. 2019c. 'ID4D: Identification for Development Brochure.' Washington, D.C.: World Bank Group. ***https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2019-05/ID4D_Overview_Brochure_English_20190508.pdf.***

World Economic Forum. 2016. 'A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity.' World Economic Forum. ***http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.***

Visit the AWS Institue ›

Access Partnership