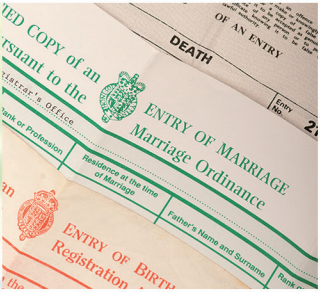
DIGITAL IDENTITY: THE ESSENTIAL GUIDE

By

Joseph J. Atick, Ph.D.

Chairman, Identity Counsel International

Co-founder and Co-Chair ID4Africa Identity Forum



Digital Identity: The Essential Guide[1]

By
Joseph J. Atick, Ph.D.
Chairman, Identity Counsel International
Co-founder and Co-Chair ID4Africa Identity Forum

THE DIGITAL REVOLUTION

Digital Identification schemes (or e-ID) have become important development initiatives in many countries around the world. This is understandable given the proven impact they have had, in many developed and pioneering countries, on governments' ability to manage their populations in order to improve the efficiency and efficacy of public service delivery, meet the growing expectation of citizens seeking to be treated as customers, and on improving national security.

In more developed states, the demand for e-ID is further fueled by the pressure to migrate to a more digital economy. Policymakers are expected to promote the creation of secure environments where connected entities access services online and transact electronically. This is the domain of e-services, which promises to make lives easier, governments and businesses more efficient, drive growth and deliver cost savings to all. The financial benefits are huge and explain why countries are accelerating their digital transformations[2].

The demand for digital identity is happening at the same time the supply side is undergoing some revolutionary changes. The expanding impact of disruptive technologies such as mobile devices, social media and more powerful ICT and big data platforms, is creating new channels for human interactions. These innovations are game-changers with broad multi-sector impact that is leading to what can only be termed the deeply *digital society.* In this brave new world, information is portable (thanks to abundant connectivity and bandwidth), accessible via the internet from anywhere anytime. It can be subjected to practically unlimited processing (thanks to abundant computational power), and consolidated from diverse sources (thanks to abundant digital data) to extract more holistic insights and actionable intelligence. Organizations can rely on data analytics to inform their decisions and to deliver qualitatively and quantitatively higher quality services attuned to the digital citizen's expectations. But for interactions in this ecosystem to function seamlessly, digital identity is key.

ROLE IN DIFFERENT COUNTRY CONTEXTS

It is easy to see why e-ID is critical in an increasingly digital society. Without it, it is difficult to ensure that services are accessed and delivered to the rightful person who has the legal authority to transact. Robust digital identity is what adds trust to an otherwise anonymous medium, devoid of accountability. Without it there would be no digital economy and its benefits would not be realizable.

Digital or Electronic Identity (e-ID)

Is a platform consisting of a collection of technologies, processes and policies that are integrated together to enable unique natural persons to prove, unambiguously and securely, who they are to an information system and to empower them to assert their legal rights in a digital context.

While the concept of e-ID is universal, the role it plays is currently different depending on country context (See Figure 1). In high income countries, it is the enabler needed to transform traditional identification practices from the physical to the digital world, motivated by convenience and e-services. In that context e-ID functions equally well as an upgrade to legacy forms of ID in the physical world.

In low income countries, that typically lack robust legacy IDs, an e-ID is primarily used for identification purposes and not e-services. It helps the country meet its identification needs in the physical world (including enhancing national security and public service administration, and making sure everyone counts) without passing through a traditional ID system first. For middle income countries, the role is somewhere in between: It delivers to the physical identity needs while at the same time supporting the emerging requisites for some e-services.

Notwithstanding the above, the absence of banking infrastructure accessible by the poor, is stimulating the adoption of alternative financial schemes, such as mobile payments and is blurring the line of demarcation for the role of e-ID in low income countries. Soon these economies may be adopting e-ID not just for identification in the physical world but for financial inclusion,

which could become a significant driver of adoption. To appreciate the potential impact it is sufficient to note that about 80% of Sub-Saharan Africa's and 65% of Latin America's adults (compared to 8% in OECD countries) are unbanked. Many are now gaining financial access through mobile money, including 16% of adults in Sub-Saharan Africa[3]. This growing use of mobile payments will create significant demand for robust, cost effective and convenient digital identification systems.

In any context, digital identity is a platform, which transcends sectors, both economic and social, and contributes to the country's political environment. For some, digital identity is a "game changer" and holds the promise to be a "poverty killer."

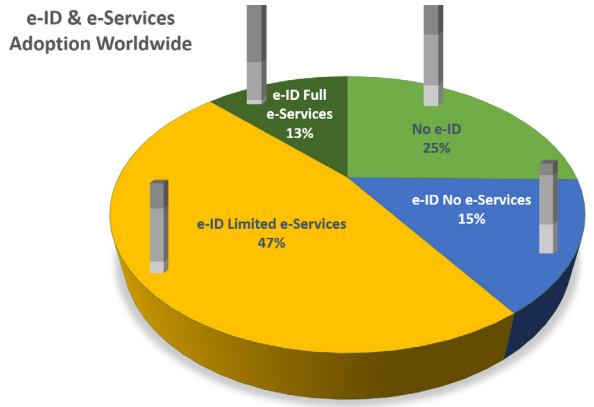


Figure 1 e-ID adoption by type of solution and by income context (graded bar with darker shade denoting higher income). It shows that 75% of the world has adopted some form of eID, but that only 13% have deployed the full range of e-Services and those are mostly in middle to high income economies. In addition 47% have already deployed some type of e-Services and that only 15% use the e-ID for identification purposes in the physical world. Graphic generated from data provided by World Bank ID4D working group.

IMPLEMENTATION ARRANGEMENTS

Broadly speaking identification systems develop in response to a specific application (elections, tax, social protection or security, pensions, health insurance etc.) and are referred to as *functional schemes*[4], or they are developed as universal multi-purpose systems capable of supporting the entire range of needs for legal identity across all applications. These are referred to as *foundational identity* schemes; their purpose is to attest, as a service, to relying third parties, to the identity of any individual.

The distinction between functional and foundational systems is not immutable over time; often functional ones evolve over time to become foundational (e.g. Bangladesh and Mexico voter ID becoming de-facto national ID). No matter what the country context is, it needs to adopt a strategy that guarantees identity-for-all, either through a universal foundational scheme or through harmonization of the multitude of existing functional systems, so that in their totality they achieve full coverage. Absence of such strategy can lead to a fragmented identity ecosystem, with a patchwork of competing schemes lacking interoperability, consistency, and with a higher risk of exclusion, as participation in functional IDs is a matter of program eligibility (e.g. children are not eligible to register in voter rosters, while middle income families are not included in poverty programs) and not a birthright as in foundational schemes.

Identity as a Utility

Operationally, under foundational schemes identity becomes a utility like energy or gas or an enabling infrastructure, like roads, that needs to be in place for the proper economic functioning of society. They aim to turn identity into commodity, available for all and for all purposes.

As for institutional arrangements, although today most foundational programs are run under ministry of interior or home affairs, increasingly they are entrusted to a stand-alone organization, the *National Identity Authority* (NIDA), independent of any line ministry (or loosely affiliated with one). NIDA could report at a cabinet level or to the presidency and is governed by a board representing the diverse identity stakeholders in the country[5]. It is tasked with implementing a unified national strategy for identification not influenced by any sectorial bias. This arrangement avoids redundancy of investment over the long term, and assures that identification needs are met consistently by design, even though it may have higher startup costs[6]. An informed identification policy, including a pathway for arriving at a universal ID given current assets and context, ultimately should achieve the right equilibrium in the identity ecosystem where supply-side (one or several institutions depending on whether model is foundational or functional) provides identification services that are consumed by the demand-side which includes the public or private sectors, alike.

DEVELOPING an e-ID SCHEME: THE TECHNICAL ASSETS

A robust identity system involves capturing the unique identity of each individual in a national identity register (see Figure 2). Once a centralized identity database is established, with unique identifying number (UIN) attributed to each individual, a government may issue official identification credentials, in the form of a national identity card, and it may also operate identity services, which verify personal identity online. In an ideal world, the national identity register can then be used across sectors, from education and healthcare to transportation and urban development, for delivery of services, both public and private. For example, a government offering safety net transfers to the country's poor can use the national identity register to help target and identify the country's poor and issue cash transfers electronically. A financial institution can use the national register to validate identity easily, thereby addressing a key aspect of Know Your Customer (KYC), and offer a host of financial services, such as opening an account, securing credit, taking deposit, or paying for services, at a bank branch, on a computer, or on a mobile phone. Immigration authorities may track who enters and exits the country, and link national passports with the unique identity of each citizen. Without a reliable way of proving one's identity, the exercise of basic people rights, the claim of entitlements, the access to a range of governmental services, and the conduct of many daily activities could be hampered. Governments play an important role in facilitating the development of such identification systems and in inculcating trust, primarily through regulations, for the broad adoption and use of identity.

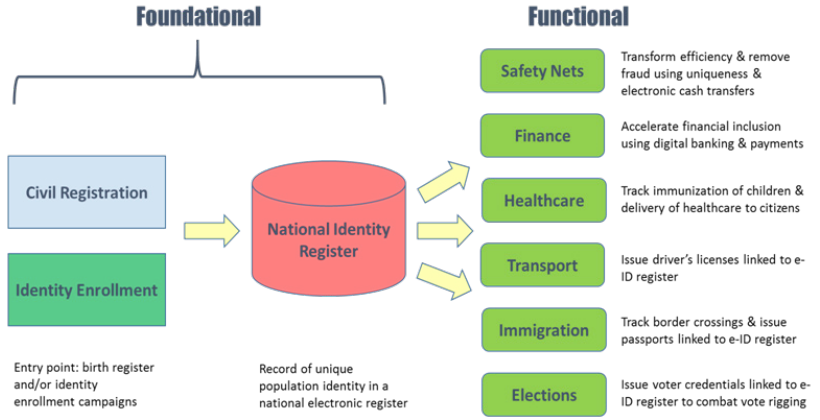


Figure 2 The interplay between foundational and functional e-ID programs in an ideal world.

It is important to emphasize that e-ID schemes, whether foundational or functional, represent a significant undertaking for most governments. They are highly technology dependent and come with all the risks associated with complex technical programs. To understand that aspect and appreciate the investments required, it is helpful to break an e-ID into its three core components, shown in Table 1.

Component	Description	Investment
Enrollment	- Involves capturing identifiers at population points of contact (permanent or temporary enrollment centers). - Includes biographic and often biometric data such as fingerprints, iris and face.	**$3-6 per person + 15-25% /yr maintenance & update of software & data[1, 2]**
Register	- Centralized databases that securely store the core identifying data. Records are often de-duplicated using biometrics and/or through linking to the birth and death registers to ensure that individuals are real and unique. - Each de-duplicated record is attributed a *Unique Identifying Number* (UIN), communicated to the citizen and that serves for life as a unified interface with public authorities. - Data is subjected to ongoing updates and validation to ensure quality and to reflect changes through life's vital events.	1. Exceptions: India Aadhaar achieved $1.16 /person with economy of scale, while one time programs such as voter registrations tend to cost almost double because of lack of leveraged permanent infrastructure. 2. Cost is inclusive of labor and equipment, database software, biometrics deduplication engines, and all the IT systems required to securely store Identity data and serve it.
Authentication & Trust Services	- Mechanisms for verifying identity at points of service offline or online. Generally known as identity credentials. - Could be secure identity cards that can be presented on demand; smart electronic cards that contain credentials on a chip (e.g. Biometrics, PIN, PKI certificates for authentication and digital signatures) that can be verified by card readers; - Could be online verification services connected to the register; - Includes trust services to secure & create audit trails.	**$1.15-$5 per ID card[1] + $0.5 /card[2] for digital certificates +$0.05-.10/yr/card maintenance** 1. Depending on physical security features, whether it is smart or not, what support for multi-applications on the card, etc. 2. Could be higher if outsourced to commercial firms instead of a national certificate authority 3. Credential cost is often born by citizen, who may be offered low-end credential or a fully featured card at higher price.

Table 1 Core components of an e-ID program and the investment needed to establish and maintain them. Source Identity Counsel International, World Bank, CDG and ID4Africa analysis.

The three core components in Table 1 and their subcomponents are integrated to produce an end-to-end identification solution. The first two participate in any ID system whether it is digital or not. While the third, its scope is enlarged to include mechanisms to authenticate identity beyond offline, in online and mobile environments, and to provide electronic trust *services* (e-TS), which include e-signatures, e-seals, and time stamps, needed to add confidence in electronic transactions (security, confidentiality, non-repudiation, audit, etc.), and to exploit full potential of e-ID as a secure medium for human-human or human-machine interactions.

THE COST DIMENSION

As can be seen from Table 1, e-ID systems can be costly (especially for sizeable populations), both in terms of up-front setup as well as ongoing operation and maintenance costs. Governments can consider potential revenue flows by offering identity services to offset the costs of e-ID development and for inducing sustainability in the e-ID operation. Public-private partnerships (PPP) can provide an avenue to relieve the fiduciary burden and has been demonstrated to be successful (especially with e-Passports) in many countries around the world. A financial and economic model, with detailed expected costs, and potential revenue streams, needs to be developed upfront.

The Investment: Example

A country of 30 million people could be looking at $90-$180 million to develop biometric population register and another $20-$60 million to credential its adults.

IDENTITY REGISTERS

Among the most fundamental assets in the country are its identity databases or registers, which allow it to know its people (see Figure 2). A register is a collection of identities, where each entry meets the following criteria:

Existence	The person exists and is alive as validated by face-to-face onboarding or other enrollment procedures (e.g. community attestation) and is not ghost or fictitious.
Uniqueness	The person can only be present once in the register. No duplicates.
Traceability	Identity is fixed for life; and even if the legal name associated with it is changed (such as upon marriage or for other reasons) it can be traced to its origin.
Link-ability	Identity must be linked to a notoriety, social or recognized legal personality (social, communal, tribal references, legal, etc.) in order for it to be empowered with the full weight of the law that recognizes its rights and responsibilities.

Table 2 Criteria that must be achieved for every entry in an identity register for it to become a good foundational database.

A register is considered a good identity database if it is inclusive and assures that each identity it contains meets the conditions in Table 2. Normally there are several types of registers, but at the foundational level the following need to be in place in order to assure that the range of identity needs of the country are met:

1. **Birth & Death or CRVS**: records all birth and death events that occur in the country as well as foreign missions. No exceptions, each life event needs to be captured. This is a legal instrument.

2. **National Population Register (NPR)**: Register of every unique individual that has the right to reside in the country (citizens, adult, children, resident foreigners, diaspora, and refugees) and their localization (address). There are many variants of the NPR depending on what information is included. Among the variants we recognize *Household Register (HHR), Family Register (FR) and Individual National Population Register (INPR)*. This is considered an administrative instrument, although often there are many laws that govern its composition and purpose.

3. **National Identity Card Register**: This is the register of people that hold a national identity card and assert their binding rights legally (e.g. adult citizens). They are often given a credential or a certificate, digital or otherwise, that allows them to transact and be recognized as a legal persons bestowed with rights and that can be subject to the full weight of the civil & criminal laws.

Ideally the above registers are linked (or interdependent as seen in Figure 2) so that identity can be traced across them. This is often not the case and represents an important opportunity for modernizing the identity assets before they can participate in a full-fledged e-ID scheme as discussed below.

ESTABLISHING UNIQUENESS

Uniqueness of the individual is at the heart of good identity management. It is what ensures that the rights and obligations of a natural person are only exercised once (one vote, one ration, one entitlement, etc.). To establish uniqueness there are several options available; which one is adopted depends on country context and development history.

The mechanisms for establishing uniqueness of identity are given in Table 3.

The Birth Register	Tracing identity to its origin. Assumes robust civil registration practices are in place and that the historical records have been digitized.
Biometrics	Such as fingerprints, iris and face. With enough biometric attributes, uniqueness can be practically assured, since within reasonable accuracy biometrics are unique to each individual. Most robust mechanism but involves cost and might encounter resistance (cultural, religious, privacy, etc.)
Know-Your-Citizen	Robust administrative procedures for building profiles of known individuals. Examples include scholastic records that document a child's educational trajectory, community attestation where the local council testifies to personal knowledge of the individual, and crowd sourcing where the community at large is invited publicly to validate the identity of its individuals, such as is often done with electoral rosters, which are published and the lists they contain are open to challenge.
Social Footprint	An individual does not exist in a vacuum in a modern society. Individual acts are recorded and accumulate in public records which are now digital. These can be used through big data analytics, mostly in developed countries, to validate that the person is real and is who they claim to be.

Table 3 Mechanisms for establishing uniqueness of identity.

THE LIFECYCLE OF AN e-ID

Putting together an e-ID program requires the execution of a project with multiple phases with varying degrees of complexity. Generally speaking these phases can be characterized as follows (Figure 3):

Data Collection: Consists of capturing identifying data and attributes, including biographic and biometric, from each living and localizable individual. This is done either at fixed points of contact (permanent enrollment centers) with the population or through mobile enrollment units. The collected data is encrypted and securely transmitted to the centralized identity authority for further processing.

Registration: Consists of validating the captured data, establishing its uniqueness through the appropriate mechanism (Table 3), attributing to it a UIN and securely storing it in a centralized identity register for later use.

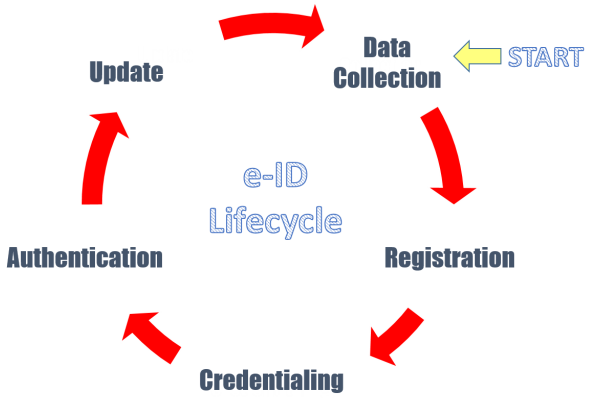


Figure 3 Digital identity lifecycle showing the onboarding of identity through data collection and registration, issuance of the appropriate credential, then using it through the authentication infrastructure and finally keeping the identity data up-to-date.

Credentialing: Consists of issuing a proof of identification to each successfully registered individual which can be asserted. In traditional identity systems (non e-ID), this involves the issuance of a printed ID document linked to the bearer through a secure personalization mechanism (e.g. photo of owner, or description securely printed on document) and carries a hallmark of trust in the form of physical security features (an official seal, hologram, etc.). For many years, this type of printed credential achieved the portability of trust. It allowed its bearer to assert his or her identity to a third-party anywhere access to the central register to verify identity was impractical. Hence it provided a general purpose mechanism for meeting society's identification needs (supported many Use-Cases).

For e-ID, credentialing is more involved and it depends on the technology platform selected for asserting identity. At one extreme of lowest cost, it could be in the form of a UIN without any token (just printed on paper, as is the case with Aadhaar in India). Identity is verified online against the identity information to which the UIN point to through a web-service

operating at the central identity register (*online identity verification on-demand*). Next level up, could be a multi-purpose single application smart card which contains the identity information of its bearer secured by a PIN or biometrics and containing digital signature certificates for authentication and/or signing (*identity verification at point of service*). A third level could be a multi-app smart card that securely holds identity as well as application specific information and other credentials (e.g. driver's permit, social program eligibility information, health and other economic data etc.). This would still contain all the usual security features such as digital certificates required for identity authentication and signature but goes way beyond. With the advent of smart mobile devices, a new medium has now become viable for carrying identity credentials. Instead of being stored on a smart card, the identity data could be kept in a secure segment of the mobile SIM card (mobile ID or m-ID).

In summary, e-ID schemes have now reached a technology regime where one can be sure that identity is unique, certified and digitally credentialed, but the options for what physical credential to use are multiple. This will continue to be the case going forward. Uniqueness of identity is driven by the requirement of trust; multiplicity of credentials is driven by the need for flexibility. Different forms of credentials are adapted for different Use Cases and hence we expect demand driven proliferation of credential types all under the framework of e-ID.

Authentication: For e-ID to be useful it needs to be verifiable, which requires an authentication infrastructure. This can consist of portals for online authentication; mobile applications for mobile-based authentication; point-of-sale (POS) terminals for smart-card or mobile-phone based authentication; and biometric terminals for biometric-based authentication; to name a few. Both government agencies (such as driver's license issuing centers, healthcare service providers, and passport issuing authorities) and private firms (such as banks and airlines) use authentication as e-government and e-commerce applications continue to grow in a country.

Authentication requires iron-clad provisions for fraud protection and high reliability and demand additional considerations in case of biometrics. At stake is the confidence of users in an identity system and in an electronic model of service delivery and transactions. The use of biometrics poses additional risks. Digital authentication, when done using PINs, passwords or SIM cards, rely on an inherent ability of these mediums to change. In

case of fraud, users are advised to promptly change PINs or passwords. A compromise of biometric information, given its inherent constancy, poses larger security risks to a user. Related to such a risk is also a determination of liability. In traditional authentication, the organization issuing the service, such as a financial service provider, assumes the sole responsibility and liability for wrongful authentication or for misuse of digital information, such as a PIN or password. In case a government agency collects biometric information and potentially provides identity services, the ownership and delineation of liability, protection of user information, and mechanisms for redress have to be clearly spelled out and governed by law.

Update: Consists of mechanisms for keeping identity data accurate and up-to-date, for example as vital information or address changes; or to allow individuals to correct inevitable errors. This requirement adds significant complexity to identity management and requires sectorial participation to ensure that identity updates are propagated across agencies if and when they happen (see below).

NATIONAL IDENTIFICATION STRATEGY

Today, the challenge faced by national governments does not lie in motivating sectorial ministries or agencies to adopt robust identification schemes in order to accelerate socio-economic development. In fact, because the interest is so high and it comes from diverse sectors, the challenge is to prevent the emergence of redundant and conflicting systems that result in wasted investments and a lost opportunity to create a coordinated service delivery platform. This potential for conflict is often reflected in the proliferation of identity registers that are not harmonized, and with the plethora of identity-based initiatives that seek to broaden the scope of some of these registers in order to have them perform functions not originally built into their mandates or in order to respond to hastily crafted and isolated mandates. One area where there is huge redundancy and continued conflict are the voter registers when they are independent of the national identity schemes. It is not uncommon to see investments being doubled and the public being biometrically enrolled multiple times because the registers are not linked. A country that has a trustworthy national identity scheme, does not need another identity database to serve as a voter register. The latter can be derived readily from the national identity[7].

In an ideal setting all major identity registers of a country do not exist in silos. Instead they are linked, so that identity is attested in a single fashion across them all. In addition there would be mechanisms in place to ensure that over time these registers remain synchronized as life vital events change. This situation leads to a *unified identification platform or framework*, a goal that policy makers need to aspire to. Within this framework, a person is known once and has to declare any update to his or her information only once and from then on it is the responsibility of the government agencies that need identifying data to recover this information.

Going from the current state of identity assets to where they need to be in order for a unified identity platform to emerge, there is a series of actions (technical and policy) that have to be performed. These can be classified into three main categories of activity, as shown Figure 4. The totality of developments identified, along with the appropriate unifying policy and legal actions represent the foundation for what can be termed as the *Unified National Identification Strategy.*

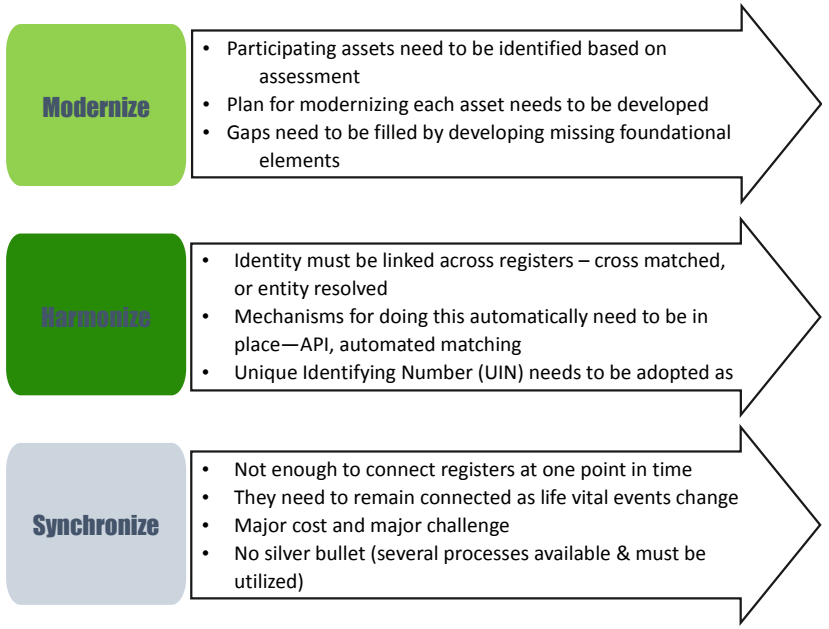


Figure 4 Developing a unified identification platform involves modernizing existing assets, harmonizing so that they are linked and synchronizing them so that a single point of update is required for capturing changes in vital information and propagating those changes across all databases. This is the technical foundation for a Unified National Identity Strategy (UNIS).

MEASURING SUCCESS

An identity scheme serves two primary stakeholders: the individuals being identified, and the institutions relying on it for customer identification. An e-ID that achieves the criteria for success listed in Table 4, becomes a critical strategic asset, that these stakeholders would not imagine functioning without it in their daily interactions.

Highly Accessible	With individual registration at near total coverage of the targeted population without exclusions.
Widely Used	Integrated into many programs by many institutions achieving high portability across them.
Highly Trusted	With robust technical measures in place to make it resilient to fraud (i.e. traceable, difficult to steal, fabricate or duplicate identity) and to create the confidence required in authenticity of transactions (data security, ID authentication and trust services).

Table 4 Success indicators for assessing an e-ID system.

In developed countries we cite, as examples, Belgium, Estonia and the Netherlands that score high on the e-ID fitness indicators. These countries have reached 100% coverage of their populations and each has several hundred highly secure and trustworthy e-services for citizens and several thousand others directed at businesses[8]. In developing countries we see India[9], Pakistan, Rwanda, Tanzania and Kenya heading in that direction and in some cases leapfrogging the e-ID initiatives of developed countries.

EVIDENCE OF IMPACT

Robust identity systems have significant impact on the functioning of many sectors of an implementing country. Some of these benefits can be quantified and considered as ROI, others are harder to assess in economic terms; nevertheless they are critical enablers for development. Due to space limitation, here we elaborate on a few areas only where e-ID systems consistently show impact:

Supporting democracy and empowering people: Nigeria in its 2015 elections used e-ID to prevent vote rigging[10]. The system enrolled about 68M voters using biometrics, prevented 4M duplicates, issued voter cards which stocked fingerprints of the rightful holder on a chip, and used card readers to authenticate voters. While there were some operational challenges at the polls, at the end of the day a successful election was conducted—all votes were cast and it was difficult to rig or contest the results in the face of the transparency brought about by digital identity. Of course this is anecdotal evidence as the experience is too recent for any systematic studies to have been done, but analysts and experts seem to agree that the impact of adopting such technology was critical in ensuring the eventual success of the elections. Nigeria is just one example. In a recent study by ID4Africa, showed that 2 out of 3 elections in Africa in 2015 used some form of biometrics and e-ID[11].

Reforming civil servants wage bill -- elimination of ghost[12] workers: The budgets of many developing countries suffer from bloated civil service wages that leave little room for investments. For example, public payroll represents 60%, 80% and 74% of the national budgets of Uganda, Zimbabwe and Ghana, respectively.[13] Reform of the wage bills is now a priority in many countries[14]. Nigeria recently implemented an e-ID for civil servants and removed about 60,000 fictitious workers to save $1 billion annually[15]. Implementing electronic wage payment system tied to an e-ID is a relatively small investment. A program to enroll half a million people costs no more than $5 million, yet in Nigeria it produced nearly 20,000% ROI in one year if government statements to the media are taken at face value. The impact of ghosts is worse in many other countries ranging from 10% to as high as 40%, as was officially estimated in Zimbabwe[16].

More efficient poverty and public service program management: Here the impact is multipronged. First e-ID allows countries to move away from market-based subsidies (which can be exploited by the non-poor) to targeted cash transfers linked to a UIN/bank-account. For example, in India's DBTL program, by implementing cash transfers to Aadhaar-linked bank accounts for the purchase of unsubsidized LPG cylinders, realizable savings are about 11-14%, or $1 billion per year when applied throughout the country.[17] This is just one of many subsidy programs in India that are being digitized impacting a total of $11.3 billion per annum[18].

Second leakages and fraud in benefits for social protection or security programs, health insurance and pension schemes due to duplicates, ghosts, quasi-ghosts and corruption can be very significant. For example, in India, an audit of beneficiaries' lists of the National Rural Employment Guarantee Scheme (NREGS) found 8.6% ghosts, 23.1% ghost person days, and only 61% of wage payments reaching eligible workers.[19] Paying beneficiaries and workers electronically introduces enormous efficiencies and prevents loss of funds. Another more recent study showed that, in one state in India, e-ID resulted in the reduction of NREGS leakages by 14% and saved, in one year, 9 times the cost of implementing the system[20]. The examples of where e-ID

has been shown effective in reducing leakages are too numerous to cite and include many programs in India, Pakistan, Indonesia, Ghana, South Africa, Egypt, Chile, Turkey, etc.

Third e-ID can enhance access to essential services (social protection, health, education, etc.) by making it easier for people to provide documentary evidence of who they are during onboarding as beneficiaries.

Improving access to financial services: A unique digital identity can make it easier for the poor to access micro-payments, micro-credit, micro-insurance, micro-pensions, and even micro-mutual funds, which are becoming available. With small, volatile incomes, the poor lack facilities for savings or insurance to protect against external shocks, such as illness, loss of a loved one, loss of job, crop failure, or to raise capital to start a small business. Mobile phones, automated teller machines (ATMs), point-of-sale (POS) devices, and agent networks provide innovative ways to access financial services, though many poor people are not able to fully benefit due to the lack of registered identity. Sub-Saharan Africa is leapfrogging developed economies in the adoptions of such innovative schemes anchored on digital identity.

Empowering Women: A digital identity can ensure that benefits meant for women, such as conditional cash transfers, actually reach women. According to the International Labor Organization (ILO), women contribute 70% of working hours globally, but receive only 10% of income flows.[21] 30 out of the bottom 40% of the population in developing countries are likely to be women. Enhancing women's incomes is recognized as one of the most effective anti-poverty programs. The money transferred to them gets spent on nutrition, education, and clothing for the family, directly impacting poverty. A good example of this is Pakistan's Benazir Income Support Program (BISP) which was launched in 2008 with the support of the World Bank as a flagship safety net program. By providing women access to the National e-ID and making BISP payments to female head of the beneficiary families, enhances women's ability to take decisions on the use of cash transfers. Since the introduction of BISP, women's registration of Computerized National Identity Cards (CNICs) has almost doubled, which can potentially open avenues for their socio-economic and political empowerment[22].

Widening the tax base: e-ID is not only used to empower citizens to exercise their rights inclusively but also to hold them responsible for their obligations, such as tax payment, which continues to be a development challenge in many nations. For example, in Tanzania, NIDA estimates that 14 million people are capable of paying tax; currently only, 1.5 million do. In India only 35 million people or 2.9% of the total population is in the taxpayers' base, according to Ministry of Finance. Adopting an e-ID with a UIN tied to financial e-services can create better transparency of citizens and their earnings, a prerequisite for a fairer tax system. Unfortunately, due to topic sensitivity, studies of the strong impact of e-ID on widening the tax base have not been widely released.

Driving Growth: ultimately a well-executed e-ID system creates a platform for commerce where transaction costs are lower and risk is mitigated since the system is resilient to fraud. Standard economic theory shows that such platforms become growth drivers. For example because of lack of robust identification many countries in Africa do not have credit bureaus and hence capital lending and financial flows, which are the prerequisites for investment growth, have been meager or nonexistent. With the advent of e-ID many African nations are now looking to develop credit bureaus (even regional ones as is the case currently in West Africa) anchored on traceable unique identity in order to stimulate commercial and consumer lending (business loans and consumer mortgages).

Other applications: The impact of e-ID programs goes beyond those areas listed above. They ultimately make public services more efficient, effective and responsive. They can improve governance and transparency, help planning, policy making, budget allocations, and human resource management. They can simplify daily lives of households and businesses by making access to public services easier, more inclusive and predictably consistent.

IMPACT ON PRIVACY

The data centric nature of e-ID, and the collection and retention of information, often deemed personal, of individuals, can be seen as an invasion of people's privacy and a significant downside of these schemes. A successful e-ID program can become pervasive over time, creating digital data trails of people's routine actions, linked to a unique and traceable identity. Thus, the effects on privacy can be further compounded. To protect people's privacy, an e-ID program has to institute strong measures,

including, but not limited to, appropriate legislation for data protection (DP) and access, and for notice and consent. The digital revolution makes a case for an independent body for data oversight and for effective enforcement of laws and regulations.

ENSURING SUCCESS

Identity programs represent important investments with significant ROI potential. But they also tend to be complex, often politicized and subject to scrutiny by media and critics. As such, failure can be costly and visible and it is not uncommon that they fail or stall before achieving their full potential.
There are many reasons why projects fail. In identity schemes failure can happen either during the execution or post launch. In the first case, the risk is primarily technical and financial, where the wrong resources are deployed against a complex project, often leading to cost overruns, mismanagement and delays or to a permanent stall in the implementation. In the second case failure becomes apparent over a longer period of time and is characterized by poor performance in the three indicators listed in Table 4. Most commonly, a scheme fails because it is not embraced by the population (low enrollment) or it does not serve the needs of a critical number of relying institutions. So it languishes and becomes obsolete for lack of continued funding and support required to maintain it. In some cases a sound program may be undermined by flaws in architecture or policy (e.g. lack of data protection) that render it untrustworthy, or by the fact that it is a closed system which over time becomes inflexible and would eventually have to be scrapped and replaced with a completely new system, instead of a simple planned upgrade.

Luckily, failure risk can be mitigated by adopting some guidelines that have emerged from the collective experience of more than a decade of e-ID implementations around the world. These include:

- *Conduct a diagnostic and adopt a Unified National Identification Strategy (UNIS)*: before any work is done on modernizing identity infrastructure of the country, a situation analysis is needed to identify the current assets that can participate in a unified identity scheme, and the current needs, and in order to uncover the challenges.

- *Enlist champions and engage all stakeholders*: The needs of all parties must be identified before irreversible design and policy actions are taken that could alienate potential users and supporters of the scheme. Put in place a multi-stakeholder project steering committee representing all sectors with various technical groups providing input, and empower its champions to conduct their mission without political interference or sectorial bias.
- *Promote ongoing cross-sectorial cooperation*: The cross-sectorial nature of e-ID requires top-level leadership and effective coordination across government agencies. Many developing countries offer a fragmented identification space, where several agencies, both public and private, compete to offer identification, in form of multiple identity cards supported by multiple identity registers. Coordinating development of an official identity across the disparate e-ID programs can be difficult and is not something that is only done once; ongoing effective coordination is required. Consider establishing a permanent strategic coordination and governance board for overseeing the ongoing needs for identification post implementation phase.
- *Adopt a technology strategy/architecture anchored on modularity and open standards*: to avoid technology and vendor lock-in and to allow for rapid corrective actions. An e-ID program relies on a large number of technological components. Luckily all are mature and have been proven effective in large scale programs. So the risk of failure is not at the core technology level; it is more likely to be the result of wrong solution architecture or implementation of the system integration. Open architecture (OA) supports good solution outcomes including interoperability, scalability and high reliability. It protects against obsolescence and makes system upgrades a normal part of the planned change management instead of a disruptive and costly event. With OA, weaknesses can be isolated and rectified by adding or replacing technology modules where and as needed without vendor intervention and without disrupting the whole system.
- *Build capacity and knowledge transfer*: The technology-centric nature of e-ID can put great demands on the technical capacity of government agencies, some of which may not directly deal with technology. Thus, leadership, governance, and capacity are important elements in the design and setup of an e-ID platform. It is imperative to develop the competent human resources and capacity to assure operations and maintenance, and support the continued evolution of the system without external dependence.

- *Limit the scope of identity data capture*: Collecting enrollment data is very costly and time consuming. Unfortunately, there is a natural tendency to want to capture a broad spectrum of information during enrollment because of pressures from the different sectorial stakeholders. This can elevate project failure risk, as data collection challenges in the field slow down the process. For a foundational program, adopt a policy for capturing a well-defined and limited set of core identifying data only that makes it clear that anything beyond that set is the responsibility of sectorial ministries that can collect information within their mandated scope of operations (e.g. health data should only be captured by ministry of health agents and only stored in their databases, not in centralized national id repositories. Similarly for tax records).
- *Promote a competitive identity marketplace*: identity needs should to be served by a robust national market which encourages multiple products, solutions and innovations from different vendors from around the world to continually compete on features, performance and price.
- *Establish supportive institutional and legislative frameworks early*: need to decide early what implementation arrangements suit the country's development needs. If it is a foundational e-ID scheme, entrust its management to a strong institution with good governance. Adopt legislations that give it the mandate to operate including collecting and storing personally identifying information. Put in place the legal framework for trust that recognizes e-ID and e-signatures as legally binding instruments.
- *Overcome obstacles to e-ID inclusion*: to ensure that no one is left behind as more services begin to rely on the scheme. This requires overcoming enrollment obstacles of certain segments of the population (children, manual laborers, disabled individuals, cultural and religious holdouts, remote individuals, etc.). The policy should make it the government's responsibility to go to the people to enroll them and not the other way round.
- *Pay attention to privacy and data protection (DP) in order to gain public trust*[23]: DP continues to take a back seat in developing countries[24], which is unfortunate since evidence shows that concerns about DP slows down adoption (e.g. Philippines, Nigeria). To win the trust of the population and achieve high engagement, a commitment to secure citizen data from hacking and to prevent its misuse has to be made along with credible enforcement policy. In addition policy is needed that defines what data is allowed to be collected at the sectorial level and for what purpose and for how long it can be kept. Luckily there are international guidelines and best practices for DP that are flexible and accommodate cultural variations in the expected norms of privacy relevant to a given country. The most commonly used guidelines in that area are known as the Fair Information Practice Principles (FIPPs) which were developed originally by the U.S. Federal Trade Commission (FTC) and were updated by the OECD[25] and today represent a good set of guidelines for data protection. The legal framework for DP should be accompanied by the establishment of the office of the Privacy Commissioner of the DP authority in order to monitor compliance and to act as an advocate for privacy rights. e-ID schemes in developed nations are trusted because of DP laws and authorities which bring transparency and recourse. For example in Belgium, people have the right to know what data is held about them and who has consulted it and to take recourse through the privacy commissioner as appropriate (Myfile).
- *Strengthen the e-ID business case by building awareness for early applications*: uptake of voluntary identity schemes tends to be slow unless there is public awareness of their utility and there are strong applications that demonstrate it[26]. Invest in early applications to stimulate the demand for e-ID simultaneous with mass enrollment campaigns, make the API for identity verification available to developers, and create awareness of value of in daily lives through outreach and media channels. The alternative is to make e-ID legally mandatory, but that does not guarantee that the public will truly embrace it or that a healthy application ecosystem will emerge.
- *Establish realistic funding*: by using the international experience as a benchmark to guide project budgets. Deviations have to be justified, as they could point to a potentially corrupt procurement practice or potential misunderstandings of true requirements.
- *Choose a credential strategy carefully*: The framework should be flexible to allow for identity verification via any medium: offline, online, and mobile. It should be cost effective and offers diversity attuned to your constituency, who may need to be verified at work, at home and on the go.

POLICY PRIORITIES IN CONTEXT

Going forward, the priorities for developing e-ID could be different in different economic contexts as shown in Figure 5. For example, low income countries should consider as high priority developing robust digital population registers that form the foundation for their identity knowledge. Those can be leveraged later through the appropriate credential strategy to meet diverse needs. Without the registers it is difficult to build e-ID. In addition, modernizing civil registration and linking to e-ID registers should be done to enhance the robustness as it connects a digital identity to its physical birth origin and ensures the deactivation of that identity upon death.

Figure 5 e-ID development priorities depending on economic context from Low to Medium to High Income Countries (LIC, MIC, and HIC).

This means that in LIC, the priority should not be to select an expensive multi-application smart card credential in the early stages of adoption of an identity scheme. This is a costly element since it is proportional to the participating population and should be done later as needs become clearer. Instead, the focus should be on the backend IT systems required to manage identity and on the identity data itself to ensure it is complete, high quality, and is adequate for assuring uniqueness and attesting to identity of all natural persons. Only after the country has developed harmonized set of identity registers can it legitimately begin to tie e-services and issue the right credentials to support them. In many cases, we have seen countries, under vendor pressure, procure costly smart cards prematurely. (In some cases millions of smart cards were delivered and remained un-personalized in warehouses and were eventually never issued and had to be written off). India should be an inspiring model for many developing countries to emulate. The country adopted a strategy that focused on enrollment and uniqueness of identity and launched the program without any smart cards or credentials, just an Aadhaar number was communicated to individuals. Only now, more than five years later, different programs are issuing application specific credentials linked to the successful Aadhaar framework and database.

On the other hand, MIC and HIC, which have robust civil registrations and digital population registers, can continue to integrate more e-services to ensure that the system has the broadest possible user base to provide a sustainable business case and revenue model. Attention to the resilience of the system against growing cyber threats and attacks is another high priority, especially in HIC, as a breach could undermine a decade of trust building and would be costly to regain.

Irrespective of country context, identity systems are national assets that need to be protected and maintained in order to serve as growth drivers.

NOTES AND REFERENCES

[1] This note benefited from work done by the author as consulting partner to the World Bank which included two public reports (Digital Identity Toolkit: A guide for stakeholders in Africa 2014 and the Digital Identity Spotlight, World Development Report 2016) as well as a large number of missions to assess identity systems of various countries around the world. The Toolkit provides further information and can be retrieved from http://documents.worldbank.org/curated/en/2014/06/20272197/digital-identity-toolkit-guide-stakeholders-africa

[2] For example, it is estimated that EU countries would save €50 billion a year by adopting electronic invoicing. Source: European Commission's Digital Agenda for Europe http://ec.europa.eu/digital-agenda/. While it is estimated that digitizing subsidy flows, could save India 1% of GDP or $20 billion a year (World Bank Development Report 2012).

[3] Source: World Bank (2014) and Wireless Intelligence (2014).

[4] We use the terminology first adopted by Gelb, A. and Clark, J. (2013). Identification for Development: The Biometrics Revolution. Working Paper 315. Center for Global Development.

[5] Examples include NIMC in Nigeria, NADRA in Pakistan, RENIEC in Peru, and NIDA in Rwanda and Tanzania.

[6] See Digital Identity Toolkit, a Guide for Stakeholders in Africa, World Bank http://documents.worldbank.org/curated/en/2014/06/20272197

[7] Elimination of this type of redundant investment, between the national ID and the voter register, should be a high priority for countries looking to modernize their identity practices and to gain the trust of their population.

[8] Source: Belgium Fedict, e-Estonia and Netherland Stelsel (http://www.fedict.belgium.be/en/; https://e-estonia.com/; http://www.e-ID-stelsel.nl/snelbuttons/english/)

[9] See Digital India initiative in general. Another example is Karnataka State, with MobileOne e-governance initiative state residents can access around 4500 services at their fingertips from their mobile phone, both private and public. Source Google Search Digital India and Karnataka MobileOne.

[10] The media reports about this recent deployment are too numerous to cite, see for example http://www.thisdaylive.com/articles/recounting-the-card-reader-experience/207491/?utm_content=buffer5c7fe&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer and http://dailyindependentnig.com/2015/04/card-reader-aided-success-presidential-poll-okoye/

[11] ID4Africa publicly tweeted internal analysis.

[12] A ghost worker is someone who is on the payroll but who does not work; it can be a real person who knowingly or not (quasi-ghost) is placed on the payroll, or a fictitious person invented by the fraud perpetrator.

[13] Source: public disclosures in media by finance ministers of several countries, monitored by Identity Counsel International and ID4Africa.

[14] Statements by ministers of finance and public officials as reported by the media. Large number of such statements can be retrieved via Google search of news archives under the keywords such as reform of civil servant wage bill, ghost workers etc. For example http://www.newsfromafrica.org/newsfromafrica/articles/art_14230.html, http://allafrica.com/stories/201409130238.html, http://www.bbc.com/news/world-africa-30137326, http://www.newzimbabwe.com/news-18552-Get+rid+of+%E2%80%98ghost+workers%E2%80%99,+says+IMF/news.aspx, http://www.news24.com/Africa/News/Tanzania-orders-probe-into-ghost-government-workers-20150329,

[15] Source statements of then Minister of Finance Dr. Ngozi Okkonjo-Iweala as reported by the media on 22 October 2014 http://www.news24.com/Africa/News/Tanzania-orders-probe-into-ghost-government-workers-20150329.

[16] Proceedings of Parliament of Zimbabwe on Feb 28, 2012.

[17] Source Barnwal, P. (2015). Curbing Leakage in Public Programs with Biometric Identification Systems: Evidence from India's Fuel Subsidies. Retrieved from: http://www.columbia.edu/~pb2442/subsidyLeakageUID.pdf

[18] **Source: Banerjee, S. (2015). From Cash to Digital Transfers in India**: The Story So Far. Retrieved from http://www.cgap.org/sites/default/files/Brief-From-Cash-to-Digital-Transfers-in-India-Feb-2015_0.pdf

[19] National Institute of Public Finance and Policy. 2012. *A cost-benefit analysis of Aadhaar*, at http://planningcommission.nic.in/reports/genrep/rep_uid_cba_paper.pdf (last accessed May 10, 2014)

[20] Banerjee, S. (2015) Opt. Cit.

[21] The Guardian. 2013. *Is empowering women the answer to ending poverty in the developing world?* At http://www.theguardian.com/global-development-professionals-network/2013/mar/26/empower-women-end-poverty-developing-world (last access May 10, 2014)

[22] A good summary of the program can be found at the World Bank website, in particular http://www.worldbank.org/en/results/2015/04/22/reaching-poorest-safety-net-pakistan

[23] e-ID systems are heavily data centric: They consume data and they generate it. Significant amount of personally identifying information (PII) is collected and centrally stored during enrollment. In addition every time an e-ID is asserted it generates transaction records which accumulate in audit trail databases. So ID management has gone from the issuance of ID cards to the management of large PII databases.

[24] Recent survey by ID4Africa initiative has revealed that 35 countries in Africa have no DP laws or authority in place. Only Benin, Burkina Faso, Côte D'Ivoire, Senegal, Gabon, Ghana, Mauritius, Morocco, South Africa and Tunisia have DP laws and authorities in place. While Angola, Care Verde, Mali have established laws not no DP Authority yet in place and Kenya, Tanzania and Uganda have only advanced to the stage of draft pending laws with their legislators.

[25] Org. for Econ. Cooperation and *Dev., OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[26] Nigeria's experience with identity systems provides great insight. Currently the country has at least three e-ID schemes: the voter register with 68M, the Banking register with 54M and the National ID with 6M enrollee as of early 2015. Enrollment in the first two was high because it was a requirement for voting and for banking, while enrollment for the National ID continues to be low since there is not yet a critical mass of applications that rely on it. A strategy that tied voter and banking to the national ID would have ensured significant uptake in the latter and would have saved the state the cost and the citizens the hassle of having to do three biometric registrations. voter and banking to the national ID would have ensured significant uptake in the latter and would have saved the state the cost and the citizens the hassle of having to do three biometric registrations.

Africa's Digital Identity Forum